Optimierungsleitfaden zur Leistung von Secure Endpoint Mac Connector

Inhalt

Einleitung

Warum müssen wir abstimmen?

Jedes Mal, wenn eine Datei auf einem Mac-Endgerät erstellt, verschoben, kopiert oder ausgeführt wird, wird ein Ereignis für diese Datei vom Betriebssystem an den Secure Endpoint Mac-Anschluss gesendet. Das Ereignis führt dazu, dass die Datei vom Connector analysiert wird. Im Rahmen des Analyseverfahrens wird in der Regel die betreffende Datei gehasht und über verschiedene Analyse-Engines sowohl auf dem Computer als auch in der Cloud ausgeführt. Es ist wichtig zu erkennen, dass diese Hashing-Vorgänge CPU-Zyklen verbrauchen.

Je mehr Dateivorgänge und -ausführungen auf einem bestimmten Endpunkt ausgeführt werden, desto mehr CPU-Zyklen und E/A-Ressourcen benötigt der Connector für das Hashing. Dem Anschluss wurden mehrere Funktionen hinzugefügt, um den Overhead zu reduzieren. Wenn beispielsweise eine Datei erstellt, verschoben oder kopiert wurde, die zuvor analysiert wurde, verwendet der Connector ein zwischengespeichertes Ergebnis. Bei bestimmten Ereignissen, z. B. bei Ausführen, bei denen Sicherheit von höchster Bedeutung ist, werden alle Ereignisse immer vollständig vom Connector analysiert. Dies bedeutet, dass Anwendungen oder Prozesse, die mehrere wiederholte Ausführen von untergeordneten Prozessen - insbesondere über einen kurzen Zeitraum - propagieren, Leistungsprobleme verursachen können. Anwendungen zu finden und auszuschließen, die untergeordnete Prozesse wiederholt mit einer höheren Geschwindigkeit ausführen, die einmal pro Sekunde die CPU-Auslastung erheblich reduziert und die Akkulaufzeit von Laptops verlängert.

Dateioperationen wie Erstellen und Verschieben haben im Allgemeinen weniger Auswirkungen als die Ausführung, aber übermäßige Dateischreibvorgänge und die temporäre Dateierstellung können zu ähnlichen Problemen führen. Eine Anwendung, die häufig in eine Protokolldatei schreibt, oder eine Anwendung, die mehrere temporäre Dateien generiert, kann dazu führen, dass Secure Endpoint viele CPU-Zyklen mit unnötiger Analyse verbraucht und für das Secure Endpoint Backend eine Menge Rauschen erzeugen kann. Die Unterscheidung von lauten Teilen legitimer Anwendungen ist ein sehr wichtiger Schritt zur Aufrechterhaltung eines produktiven und sicheren Endgeräts.

Dieses Dokument soll dabei helfen, die Dateioperationen (Erstellen, Verschieben und Kopieren) zu unterscheiden und auszuführen, die negative Auswirkungen auf die Leistung des Daemons haben und CPU-Zyklen vergeuden. Durch die Identifizierung dieser Datei- und Verzeichnispfade

können Sie die entsprechenden Ausschlussgruppen für Ihr Unternehmen erstellen und verwalten.

Sie können Ihren Richtlinien, die von Cisco verwaltet werden, vordefinierte Ausschlusslisten hinzufügen, um eine bessere Kompatibilität zwischen dem Secure Endpoint Connector und Antivirus-, Sicherheits- oder anderer Software zu gewährleisten. Diese Listen sind auf der Seite Ausschlüsse in der Konsole als von Cisco gepflegte Ausschlüsse verfügbar.

Abstimmungstypen

Es stehen drei Arten von Ausschluss-Tuning-Optionen zur Verfügung:

1. **Tuning vor der Installation: Dies kann vor der Installation des Secure Endpoint Mac Connectors erfolgen. Sie erhalten einen genaueren Einblick in die Anwendungen und Pfade, die am meisten auf Ihrem Computer laufen. Es ist jedoch ein sehr lauter Prozess, bei dem der Benutzer selbst eine Analyse und Aggregation durchführen muss.**
2. **Support Tool Tuning**: Dies kann nach der Installation des Mac Connectors erfolgen und kann auf jedem Endgerät ohne zusätzliche Binärdateien durchgeführt werden. Es führt einen begrenzten Rückblick durch und eignet sich hervorragend zur Identifizierung von Anwendungen, die Probleme verursachen.
3. **Procmon Tuning** - Bei diesem Vorgang muss auch der Anschluss installiert sein, aber es muss auch das Procmon Binärprogramm, unser benutzerdefiniertes Tuning-Tool, verwendet werden. Es handelt sich im Wesentlichen um eine ausgereiftere Version der Unterstützungswerkzeug-Optimierungsfunktion. Für diese Methode ist der größte Konfigurationsaufwand erforderlich. Sie liefert jedoch die besten Ergebnisse.

1. Optimierung vor der Installation

Tuning vor der Installation ist die einfachste Form der Optimierung und wird hauptsächlich über die Befehlszeile in einer Terminal-Sitzung durchgeführt.

Für neuere Mac von OS X El Capitan müssen Sie zuerst booten, um den Wiederherstellungsmodus (command-r) wiederherzustellen, während Sie booten und den Schutz für dtrace deaktivieren:

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

Führen Sie folgende Schritte aus, um zu überprüfen, welche Dateiausführungen am häufigsten vorkommen:

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

Dies zeigt im Allgemeinen an, welche Anwendungen immer wieder ausgeführt werden. Viele Bereitstellungsanwendungen führen Skripts aus oder führen Binärdateien in kurzen Intervallen aus, um die Unternehmenssoftware-Richtlinien aufrechtzuerhalten. Alle Anwendungen, die mit einer Geschwindigkeit von mehr als einmal pro Sekunde ausgeführt werden oder die mehrmals in kurzen Spitzen ausgeführt werden, sollten als gute Ausschlusskandidaten betrachtet werden.

Führen Sie den folgenden Befehl aus, um zu überprüfen, welche Dateivorgänge am häufigsten ausgeführt werden:

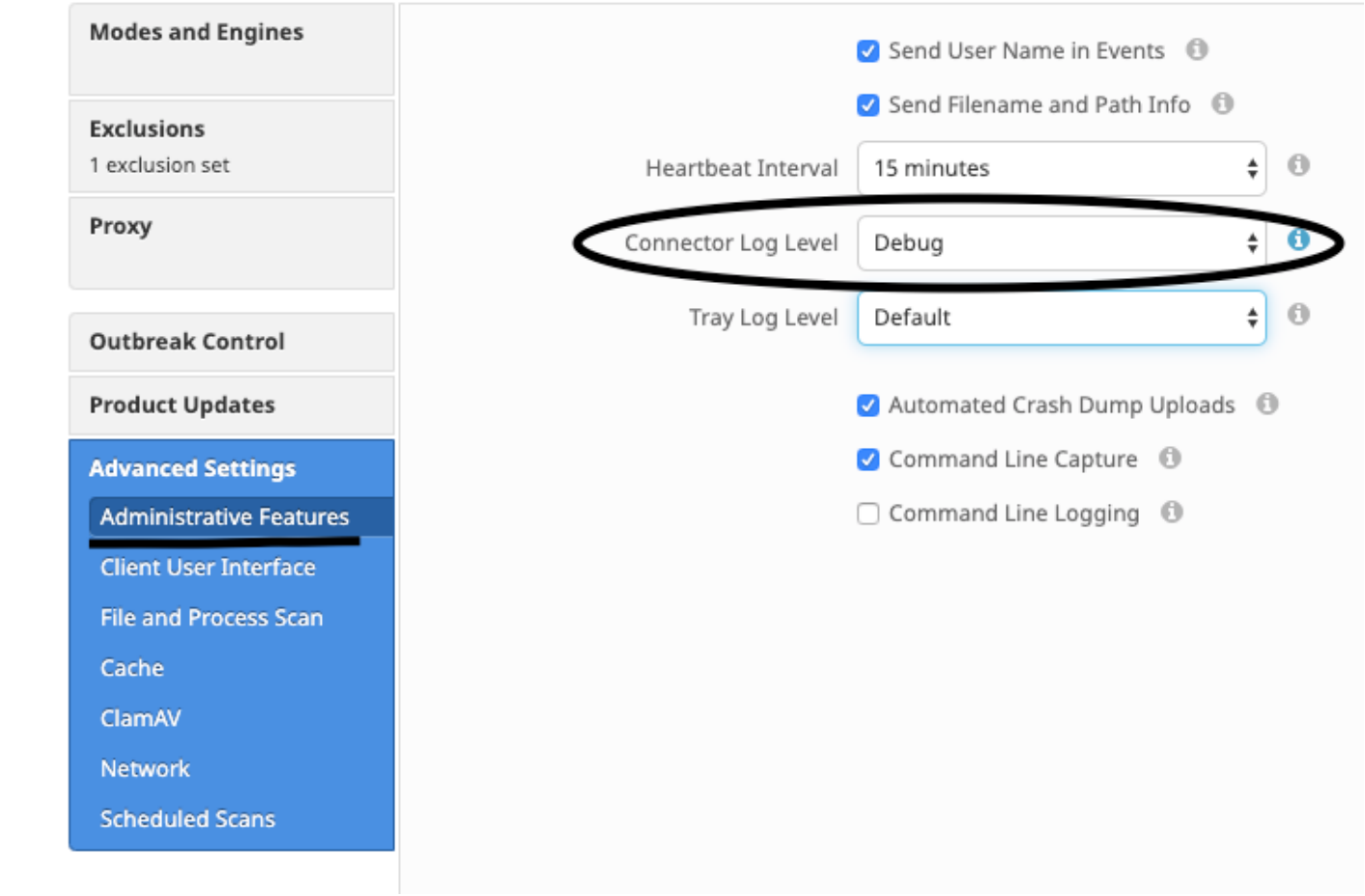
```
$ sudo iosnoop | perl -pe 'use POSIX strftime; print strftime "[%Y-%m-%d %H:%M:%S] ", localtime'
```

Sie sehen sofort, in welche Dateien die meisten geschrieben werden. Oft handelt es sich dabei um Protokolldateien, auf die durch Ausführung von Anwendungen geschrieben wird, um Sicherungssoftware, um Kopierdateien oder um E-Mail-Anwendungen, die temporäre Dateien schreiben. Darüber hinaus ist eine gute Faustregel, dass alles mit einer Protokoll- oder Journaldateierweiterung als geeigneter Ausschlusskandidat betrachtet werden sollte.

2. Support-Tool Anpassung

Aktivieren der Debug-Protokollierung

Der Connector-Daemon muss in den Debug-Protokollierungsmodus gesetzt werden, bevor die Unterstützung für die Dateioptimierung beginnt. Dies erfolgt über die Konsole für sichere Endgeräte, über die Richtlinieneinstellungen des Connectors unter *Management -> Policies (Verwaltung -> Richtlinien)*. Wählen Sie die Richtlinie aus, bearbeiten Sie die Richtlinie, und gehen Sie in der Seitenleiste *Erweiterte Einstellungen zum* Abschnitt *Verwaltungsfunktionen*. Ändern Sie die Einstellung *für den Anschluss Log Level (Protokollstufe*) in **Debug**.



Weiter, Ihre Richtlinie speichern. Sobald Ihre Policy gespeichert wurde, Sicherstellen, dass synchronisiert wurdehronisiert an cAnschluss. Führen Sie den cAnschluss in diesem Modus für mindestens 15-20 Minuten vor der Fortsetzung der Rest der Optimierung.

HINWEIS: Wenn Ihre Abstimmung abgeschlossen ist, vergessen ändern Sie *Anschlussprotokollebene* Zurücksetzen auf **Standard** damit cAnschluss Laufbahnen in seine effizienteste und Effektivmodus.

Ausführen des Support-Tools

Diese Methode umfasst die Verwendung des Support-Tools, einer Anwendung, die mit dem Secure Endpoint Mac-Anschluss installiert ist. Sie können den Zugriff über den Ordner "Applications" (Anwendungen) aufrufen, indem Sie auf /Applications->Cisco Secure Endpoint->Support Tool.app doppelklicken. Dadurch wird ein vollständiges Support-Paket generiert, das zusätzliche Diagnosedateien enthält.

Ein Alternative, und schneller, die Methode ist, folgende Befehlszeile von eine Terminal Sitzung:

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

Dies führt dazu, dass eine deutlich kleinere Unterstützungsdatei nur die relevanten Tuning-Dateien enthält.

Das Support-Tool generiert auf Ihrem Desktop eine ZIP-Datei, die zwei Tuning-Unterstützungsdateien enthält: fileops.txt und Execs.txt. fileops.txt enthält eine Liste der am häufigsten erstellten und geänderten Dateien auf Ihrem Computer. Execs.txt enthält die Liste der am häufigsten ausgeführten Dateien. Beide Listen sind nach Anzahl der Scans sortiert, d. h. die am häufigsten gescannten Pfade werden oben in der Liste angezeigt.

Lassen Sie den Connector 15-20 Minuten lang im Debugmodus laufen, und führen Sie dann das Support-Tool aus. Eine gute Faustregel ist, dass alle Dateien oder Pfade, die durchschnittlich 1000 Treffer oder mehr in dieser Zeit sind gute Kandidaten, ausgeschlossen werden.

Ausschlüsse für Pfad, Platzhalterzeichen, Dateinamen und Dateierweiterungen erstellen

Eine Möglichkeit, mit Pfadausschlussregeln zu beginnen, besteht darin, die am häufigsten gescannten Datei- und Ordnerpfade aus fileops.txt zu finden und dann die Erstellung von Ausschlussregeln für diese Pfade in Betracht zu ziehen. Überprüfen Sie nach dem Herunterladen der Richtlinie die CPU-Auslastung. Es kann 5 bis 10 Minuten dauern, bis die Richtlinie aktualisiert ist, bevor Sie feststellen, dass die CPU-Auslastung abnimmt, da es für den Daemon Zeit dauern kann, den Vorgang abzufangen. Wenn immer noch Probleme auftreten, führen Sie das Programm erneut aus, um zu sehen, welche neuen Pfade Sie beobachten.

- Eine gute Faustregel ist, dass alles mit einer Protokoll- oder Journaldateierweiterung als geeigneter Ausschlusskandidat betrachtet werden sollte.

Erstellen von Prozessausschlüssen

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).
Best Practices für Prozessausschlüsse finden Sie unter:Sicheres Endgerät: Prozessausschlüsse in MacOS und Linux

Ein gutes Tuning-Muster besteht zunächst darin, die Prozesse zu identifizieren, bei denen ein hohes Volumen an ausführbaren Dateien von Execs.txt ausgeführt wird, den Pfad zur ausführbaren Datei zu finden und einen Ausschluss für diesen Pfad zu erstellen. Es gibt jedoch einige Prozesse, die nicht einbezogen werden sollten, darunter:

- Allgemeine Dienstprogramme - Es wird nicht empfohlen, allgemeine Dienstprogramme auszuschließen (z. B.: usr/bin/grep) ohne Berücksichtigung der folgenden Punkte. Der Benutzer kann bestimmen, welche Anwendung den Prozess aufruft (z. B.: Suchen Sie den übergeordneten Prozess, der grep ausführt), und schließen Sie den übergeordneten Prozess aus. Dies sollte nur dann erfolgen, wenn der übergeordnete Prozess sicher in einen Prozessausschluss umgewandelt werden kann. Wenn der Elternausschluss für Kinder gilt, werden auch Aufrufe von Kindern aus dem Elternprozess ausgeschlossen.Der Benutzer, der den Prozess ausführt, kann bestimmt werden. (Bsp.: Wenn ein Prozess auf einem hohen Volumen von Benutzer "root" aufgerufen wird, kann der Prozess ausgeschlossen werden, aber nur für den angegebenen Benutzer "root", so kann Secure Endpoint die Ausführung eines bestimmten Prozesses durch einen Benutzer überwachen, der nicht "root" ist.)**HINWEIS: Ausschlüsse von Prozessen sind neu in den Connector-Versionen 1.11.0 und neuer. Aus diesem Grund können allgemeine Dienstprogramme als Pfadausschluss in Connector Version 1.10.2 und älteren Versionen verwendet werden. Diese Vorgehensweise wird jedoch nur empfohlen, wenn ein Leistungskompromiss unbedingt erforderlich**

ist.

Für Ausschlüsse von Prozessen ist es wichtig, den übergeordneten Prozess zu finden. Sobald der Parent Process bzw. User des Prozesses gefunden wurde, kann der Benutzer den Ausschluss für einen bestimmten Benutzer erstellen und den Prozessausschluss auf Kindprozesse anwenden, was wiederum laute Prozesse ausschließt, die nicht selbst in Prozessausschlüsse umgewandelt werden können.

Übergeordneter Prozess identifizieren

1. Identifizieren Sie in der Datei Execs.txt den Prozess mit hohem Volumen (z. B.: /bin/rm).
2. Öffnen Sie ampdaemon.log aus dem Support-Paket, entpacken Sie syslog.tar, und folgen Sie dem Pfad /Library/Logs/Cisco/ampdaemon.log (nur im Support-Paket verfügbar, nicht aus einem Support-Paket, das mit den Standardoptionen generiert wurde).
3. Suchen Sie ampdaemon.log, um den Prozess auszuschließen. Suchen Sie die Protokollzeile, die die Ausführung des Prozesses anzeigt (z. B.: 19. Aug. 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. Identifizieren des übergeordneten Prozesses mithilfe einer der folgenden Methoden: Identifizieren Sie den Pfad des übergeordneten Prozesses, der dem auszuschließenden Prozess folgen kann (z. B.: [/bin/rm] [*Parent Process path*]).Wenn das Protokoll den Pfad für den übergeordneten Prozess nicht enthält, identifizieren Sie die übergeordnete Prozess-ID im `PP:`-Abschnitt der Protokollzeile (z. B.: PP:3200).
5. Wiederholen Sie die Schritte 3 und 4, um entweder den übergeordneten Pfad oder die übergeordnete Prozess-ID zu ermitteln. Setzen Sie diesen Prozess fort, bis entweder kein übergeordneter Prozess oder die übergeordnete Prozess-ID = 1 (z. B.: PP:1).
6. Wenn die Prozessstruktur bekannt ist, suchen Sie nach dem Programmpfad, der die meisten oder alle auszuschließenden Vorgänge abdeckt und die Anwendung eindeutig identifiziert. Dadurch wird das Risiko minimiert, dass Vorgänge, die von einer anderen Anwendung ausgeführt werden, versehentlich ausgeschlossen werden.

Benutzer des Prozesses identifizieren

1. Befolgen Sie die Schritte 1-3 zur Identifikation des übergeordneten Prozesses von oben.
2. Identifizieren Sie Benutzer eines Prozesses mithilfe einer der folgenden Methoden: Suchen Sie die Benutzer-ID des angegebenen Prozesses von `U:` in der Protokollzeile (z. B.: U:502).Führen Sie im Terminal-Fenster den folgenden Befehl aus: `dscl . Liste /Users UniqueID | grep #`, wobei # die Benutzer-ID ist.Die Ausgabe sollte ähnlich wie bei `Benutzername 502` angezeigt werden, wobei `Benutzername` der Benutzer des angegebenen Prozesses ist.
3. Dieser Benutzername kann einem Prozess-Ausschluss unter der Kategorie Benutzer hinzugefügt werden, um den Umfang des Ausschlusses zu reduzieren, der für bestimmte Prozessausschlüsse wichtig ist. **HINWEIS: Wenn der Benutzer eines Prozesses der lokale Benutzer des Computers ist und dieser Ausschluss auf mehrere Computer mit unterschiedlichen lokalen Benutzern angewendet werden muss, muss die Benutzerkategorie leer gelassen werden, damit der Prozessausschluss auf alle Benutzer angewendet werden kann.**