Secure Endpoint Mac Connector - hoogwaardige tunnelgids

Inhoud

Inleiding

Waarom moeten we afstemmen?

Elke keer dat een bestand wordt gemaakt, verplaatst, gekopieerd of uitgevoerd op een Mac-eindpunt wordt een gebeurtenis voor dat bestand vanuit het besturingssysteem naar de Secure Endpoint Mac-connector verzonden. De gebeurtenis levert een bestand op dat door de connector wordt geanalyseerd. Het analyseproces omvat over het algemeen het hasken van het betreffende bestand en het doorlopen van het door verschillende analysemotoren, zowel op de computer als in de cloud. Het is belangrijk om te erkennen dat deze handeling van het slaan van beelden CPU-cycli vereist.

Hoe meer bestandsbewerkingen en uitvoeringen op een bepaald eindpunt, des te meer CPU-cycli en I/O-bronnen de connector nodig zal hebben voor het hashing. Er zijn verschillende functies aan de connector toegevoegd om de overhead te verminderen. Als bijvoorbeeld een bestand dat wordt gemaakt, verplaatst of gekopieerd eerder is geanalyseerd, zal de connector een gecached resultaat gebruiken. In het geval van bepaalde gebeurtenissen, zoals executies waar veiligheid van het allergrootste belang is, worden alle gebeurtenissen echter altijd volledig geanalyseerd door de connector. Dit betekent toepassingen of processen die meerdere, repetitieve executies van kinderprocessen propageren - vooral over een korte periode - kunnen er prestatiekwesties ontstaan. Toepassingen vinden en uitsluiten die meerdere kinderprocessen uitvoeren met een hogere snelheid dan één keer per seconde, kan uw CPU-gebruik aanzienlijk verminderen en de accuduur op laptops verhogen.

Bestandsbewerkingen zoals maken en verplaatsen hebben over het algemeen minder effect dan uitvoeren, maar excessieve bestandstypen en tijdelijke bestandsindeling kan leiden tot soortgelijke problemen. Een toepassing die regelmatig naar een logbestand schrijft, of een toepassing die meerdere tijdelijke bestanden genereert, kan Secure Endpoint veroorzaken om veel CPU-cycli te consumeren met onnodige analyse en kan veel ruis creëren voor het Secure Endpoint-backend. Het onderscheiden van delen van legitieme applicaties die ruis veroorzaken is een zeer belangrijke stap in het behoud van een productief en veilig eindpunt.

Dit document heeft als doel te helpen bij het onderscheiden van de bewerkingen van bestanden (maken, verplaatsen en kopiëren) en uitvoeringen die een negatief effect hebben op de prestaties van de daemon en de verspilling van CPU-cycli. Door deze bestanden en directory paden te identificeren kunt u de juiste uitsluitingssets voor uw organisatie maken en onderhouden.

U kunt vooraf gemaakte uitsluitingslijsten aan uw beleid toevoegen die door Cisco worden onderhouden om een betere compatibiliteit tussen de Secure Endpoint-connector en het antivirus, de beveiliging of andere software te bieden. Deze lijsten zijn beschikbaar op de pagina Uitsluitingen in de console als Cisco-Behielden uitsluitingen.

Typen tuning

Er zijn drie soorten opties voor het afstemmen van uitsluitingen beschikbaar:

1. **Pre-Installeer Tuning - dit kan worden gedaan voordat u de Secure Endpoint Mac-connector installeert. U krijgt dan de schoonste blik op welke toepassing en paden het drukste op uw machine zijn. Maar het is een zeer lawaaierig proces en vereist dat de gebruiker een beetje analyse en aggregatie op zichzelf maakt.**
2. **Ondersteuning van** snijpad - dit kan worden gedaan nadat de Mac-connector is geïnstalleerd en kan worden uitgevoerd op elk eindpunt zonder extra binaire structuur. Hij doet een beperkte terugblik en is geweldig voor het identificeren van problematische toepassingen.
3. **Aanpassen** - dit proces vereist ook dat de connector wordt geïnstalleerd, maar vereist ook het gebruik van het Procmon binaire, onze aangepaste tuning tool. Het is in wezen een geavanceerdere versie van de Support Tool-tuning functie. Voor deze methode is de grootst mogelijke configuratie vereist; het biedt echter wel de beste resultaten .

1. Aangepaste installatie

Pre-Install Tuning is de meest elementaire vorm van tuning en wordt voornamelijk uitgevoerd via de opdrachtregel in een eindsessie.

Voor een nieuwere mac van OS X El Capitan moet u eerst beginnen om de modus (commando-r) te herstellen terwijl u de beveiliging tegen overtrekken start en schakelt u de beveiliging voor overtrekken uit:

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

Om te inspecteren welke bestanden het meest worden uitgevoerd voert u het volgende uit:

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

Dit zal over het algemeen tonen welke toepassingen telkens opnieuw worden uitgevoerd. Vele provisioningtoepassingen zullen scripts uitvoeren of binaries uitvoeren in korte intervallen om software beleid van het bedrijf te onderhouden. Aanvragen waarvan wordt vastgesteld dat zij met een hogere snelheid dan eens per seconde worden uitgevoerd, of die meerdere keren worden uitgevoerd in korte uitbarstingen, moeten worden beschouwd als een goede kandidaat voor uitsluiting.

Om te inspecteren welke bestandsbewerkingen het meest voorkomen, voert u de volgende opdracht uit:

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

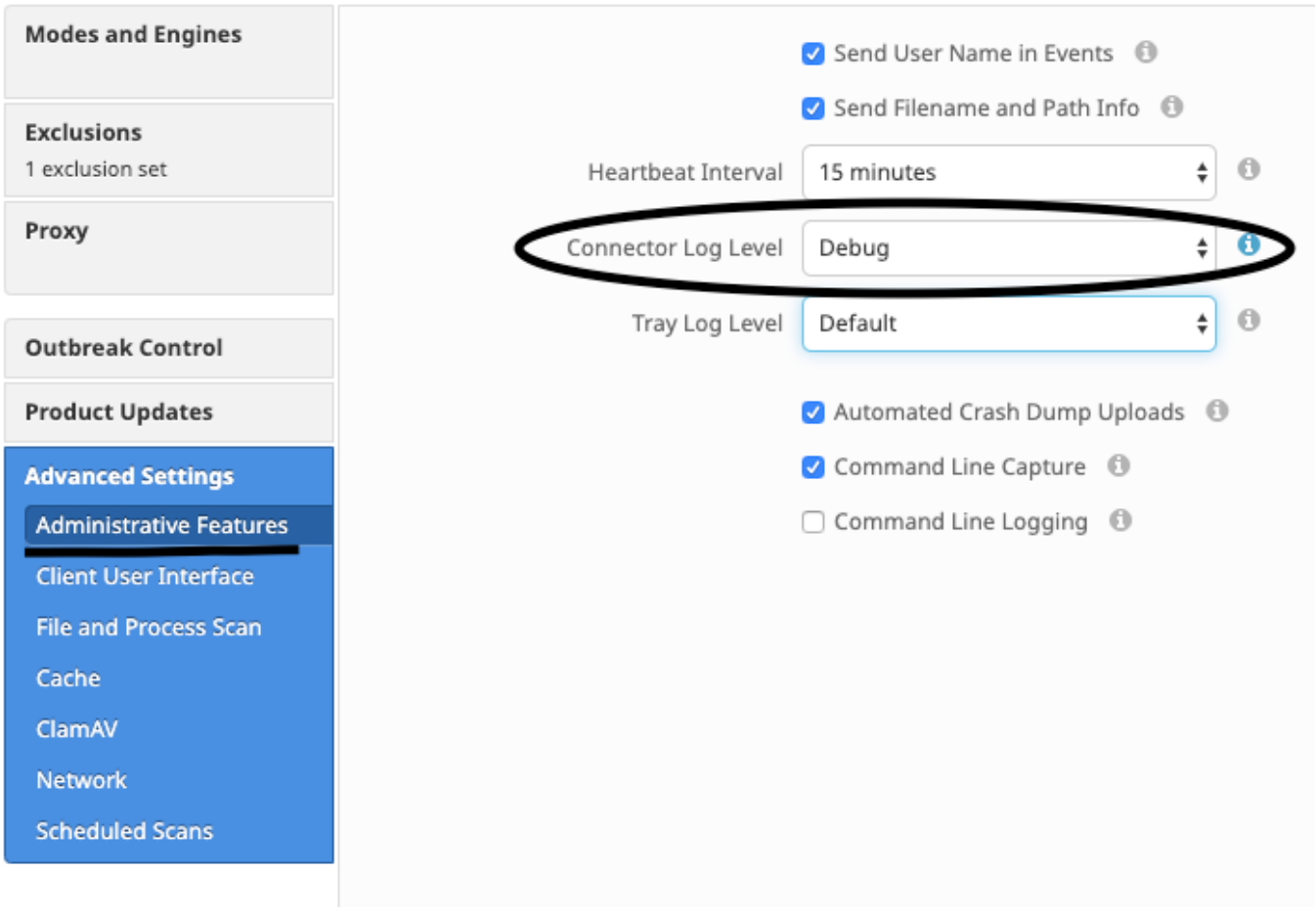
U zult onmiddellijk zien welke bestanden op de meeste bestanden worden geschreven. Dit zijn meestal logbestanden die worden geschreven door toepassingen, reservesoftware, het kopiëren

van bestanden of e-mailtoepassingen die tijdelijke bestanden schrijven. Bovendien is het een goede regel dat alles met een log- of een tijdschrift-bestandsextensie als een geschikte uitsluitingskandidaat moet worden beschouwd.

2. Ondersteuningsinstrument Tuning

Debug-vastlegging inschakelen

De naam van de connector moet in de Debug Logging-modus worden geplaatst voordat u een begin maakt met het afstemmen van ondersteuningsbestanden. Dit gebeurt via de Secure Endpoint-console, via de beleidsinstellingen van de connector bij *Management ->-beleid*. Selecteer het beleid, Bewerk het beleid en ga naar de sectie *Administratieve eigenschappen* onder de knoppenbalk *Geavanceerde instellingen*. Wijzig de instelling *Log Level* van de *aansluiting* tot **debug**.



Volgende, bespaart u uw beleid . Wanneer uw beleid is opgeslagen, controleer of het sync isgemarteld aan cconnector. Draai de toets caansluiting in deze modus minstens 15-20 minuten voordat de behandeling wordt voortgezet de rest van de stemming.

OPMERKING: Wanneer het afstemmen is voltooid, doe het dan niet vergeten de *aansluitingsniveau* terugplaatsen naar **Standaard** zodat caansluiting lopen in haar meest efficiënt en effectieve modus.

Ondersteunende tool uitvoeren

Deze methode omvat het gebruik van het Ondersteuningsgereedschap, een toepassing die met

de Secure Endpoint Mac-connector is geïnstalleerd. Het programma is bereikbaar in de map Toepassingen door te dubbelklikken op <Application>Cisco Secure Endpoint->Support Tool.app. Dit zal een volledig steunpakket genereren dat extra diagnostische bestanden bevat.

Een alternatief, en sneller, methode is om de volgende opdrachtregel van a terminal zitting :

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

Dit zal resulteren in een veel kleiner ondersteuningsbestand dat alleen de relevante tuning-bestanden bevat.

Beide manieren waarop u ervoor kiest om dit te doen, genereert Support Tool een zip-bestand op uw bureaublad dat twee tuning-ondersteuningsbestanden bevat: fileops.txt en execus.txt. fileops.txt bevat een lijst van de meest gemaakte en aangepaste bestanden op uw machine. execus.txt zal de lijst van de meest vaak uitgevoerde bestanden bevatten. Beide lijsten worden gesorteerd door middel van een scan-telling, wat de meest gescande paden betekent, verschijnen boven in de lijst.

Laat de connector 15-20 minuten in de Debug-modus lopen en voer vervolgens het ondersteuningsgereedschap uit. Een goede vuistregel is dat alle bestanden of paden die gemiddeld 1000 hits of meer in die tijd zijn, goede kandidaten zijn die moeten worden uitgesloten.

Uitsluitingen voor pad, jokerteken, bestandsnaam en bestandsextensie maken

Eén manier om te beginnen met de regels van de Uitsluiting van het Pad is het vaakst gescande bestand en mappenpaden vinden van velden.txt en overwegen dan om uitsluitingsregels voor die paden te creëren. Nadat het beleid is gedownload, controleert u het nieuwe CPU-gebruik. Het kan 5 tot 10 minuten duren nadat het beleid is bijgewerkt voordat u de CPU-gebruiksdaling opmerkt, aangezien het tijd kan duren voordat de datum wordt ingehaald. Als u nog problemen ziet, voert u het gereedschap opnieuw uit om te zien welke nieuwe paden u waarneemt.

- Een goede vuistregel is dat alles met een log- of een tijdschrift-bestandsextensie als een geschikte uitsluitingskandidaat moet worden beschouwd.

Procesuitsluitingen maken

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).
Zie voor beste praktijken met betrekking tot procesuitsluitingen:Secure-eindpunt: Procesuitsluitingen in macOS en Linux

Een goed stempatroon is eerst het identificeren van de processen met een hoog volume executies van execus.txt, het pad naar het uitvoerbaar vinden en een uitsluiting voor dit pad creëren. Er zijn echter enkele processen die niet moeten worden opgenomen, zoals:

- Algemene hulpprogramma's - Het wordt niet aanbevolen algemene gebruiksprogramma's uit te sluiten (bijvoorbeeld: usr/bin/grep) zonder rekening te houden met het volgende: De gebruiker kan bepalen welke toepassing het proces oproept (bijvoorbeeld: het ouderproces vinden dat grijp uitvoert) en het ouderproces uitsluiten. Dit dient alleen te gebeuren als en alleen als het moederproces veilig kan worden afgesloten met een procesuitsluiting. Als de ouderuitsluiting van toepassing is op kinderen, dan worden de oproepen naar kinderen van het moederproces ook uitgesloten.De gebruiker die het proces uitvoert, kan worden vastgesteld. (ex: Als een proces bij een hoog volume door gebruiker "root" wordt opgeroepen, kan het proces worden uitgesloten, maar alleen voor de gespecificeerde user 'root', dan kan Secure Endpoint de uitvoering van een bepaald proces controleren door een gebruiker die geen 'root' is.**LET OP: Procesuitsluitingen zijn nieuw in verbindingsversies 1.11.0 en nieuwer. Daarom kunnen algemene hulpprogramma's worden gebruikt als Pad-uitsluiting in connector versies 1.10.2 en ouder. Deze praktijk wordt echter alleen aanbevolen wanneer een prestatietransactie absoluut noodzakelijk is.**

Het ouder maken is belangrijk voor procesuitsluitingen. Zodra het Parent-proces en/of de gebruiker van het proces zijn gevonden, kan de gebruiker de uitsluiting voor een specifieke gebruiker creëren en de procesuitsluiting toepassen op kinderprocessen, waardoor lawaaiprocessen die zelf niet in procesuitsluitingen kunnen worden omgezet, worden uitgesloten.

Parkeerproces identificeren

1. Identificeer hoog volume proces (bijvoorbeeld: /bin/rm).
2. Open ampdaemon.log uit het ondersteuningspakket, unzip syslog.tar, dan volgt pad /Library/Logs/Cisco/ampdaemon.log (alleen beschikbaar in het ondersteuningspakket, niet van een ondersteuningspakket dat met de standaardopties gegenereerd is).
3. Zoek op ampdaemon.log dat dit proces is uitgesloten. Vind de loglijn die de procesuitvoering (bijvoorbeeld: 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. Identificeer het moederproces aan de hand van een van de volgende methoden: Identificeer het snijpad van het moederproces dat het pad van het uit te sluiten proces kan volgen (bijvoorbeeld: [/bin/rm] [*Parent Procespad*]).Als het logbestand het snijpad van Parent niet bevat, moet u de `PP`-ID van Parent `verwerken:` onderdeel van de loglijn (bijvoorbeeld: blz. 3200).
5. Wanneer u het ouderpad of de ID Parent Processing gebruikt, herhaalt u stap 3 en 4 om de ouder van het huidige Parent-proces te bepalen. Ga door met dit proces totdat geen ouder kan worden bepaald of de ID van het moederproces = 1 (bijvoorbeeld: blz. 1).
6. Nadat de procesboom bekend is, zoekt u het programmapad dat de meeste of alle bewerkingen bestrijkt die moeten worden uitgesloten, en identificeert u de toepassing op een unieke manier. Dit minimaliseert de kans om onbedoeld transacties uit te sluiten die door een andere toepassing worden uitgevoerd.

Gebruiker van proces identificeren

1. Volg stap 1-3 van het identificeren van het ouder proces van bovenaf.
2. Identificeer gebruiker van een proces met behulp van een van de volgende methoden: Vind de Gebruiker ID van het bepaalde proces in `U:` in de loglijn (bijvoorbeeld: U: 502).Voer in het Terminalvenster de volgende opdracht in: `dscl. lijst/gebruikers unieke ID | grep #`, waarbij # de gebruiker-ID is.U dient uitvoer vergelijkbaar te zien met: `Gebruikersnaam 502`, waarbij `Gebruikersnaam` de Gebruiker van het opgegeven proces is.
3. Deze gebruikersnaam kan worden toegevoegd aan een procesuitsluiting onder de gebruikerscategorie om het toepassingsgebied van de uitsluiting te beperken, hetgeen voor bepaalde procesuitsluitingen belangrijk is. **OPMERKING: Als de gebruiker van een proces de lokale gebruiker van de machine is, en deze uitsluiting van toepassing moet zijn op meerdere machines met verschillende lokale gebruikers, moet de categorie Gebruiker leeg gelaten worden om de Procesuitsluiting op alle gebruikers van toepassing te laten zijn.**