Guia de ajuste de desempenho do conector Mac de endpoint seguro

Contents

Introduction

Por que precisamos de sintonizar?

Cada vez que um arquivo é criado, movido, copiado ou executado em um endpoint Mac, um evento para esse arquivo é enviado do sistema operacional para o conector Mac do Secure Endpoint. O evento faz com que o arquivo seja analisado pelo conector. O processo de análise geralmente envolve o hashing do arquivo em questão e sua execução através de diferentes mecanismos de análise, tanto no computador quanto na nuvem. É importante reconhecer que esse ato de hash consome ciclos de CPU.

Quanto mais operações de arquivos e execuções ocorrerem em um determinado endpoint, mais ciclos de CPU e recursos de E/S o conector exigirá para o hashing. Há vários recursos que foram adicionados ao conector para reduzir a sobrecarga. Por exemplo, se um arquivo que está sendo criado, movido ou copiado tiver sido analisado anteriormente, o conector usará um resultado em cache. No entanto, no caso de alguns eventos, como execuções em que a segurança é fundamental, todos os eventos são sempre completamente analisados pelo conector. Isso significa que aplicativos ou processos que propagam várias execuções repetitivas de processos filho - especialmente em um curto período de tempo - podem causar problemas de desempenho. Encontrar e excluir aplicativos que executam repetitivamente processos filho a uma taxa maior que uma vez por segundo pode reduzir significativamente o uso da CPU e aumentar a autonomia da bateria em laptops.

Operações de arquivos como criação e movimentação geralmente têm menos impacto que as execuções, mas gravações excessivas de arquivos e criação temporária de arquivos podem resultar em problemas semelhantes. Um aplicativo que grava com frequência em um arquivo de log ou que gera vários arquivos temporários pode fazer com que o Secure Endpoint consuma muitos ciclos de CPU com análise desnecessária e pode criar muito ruído para o backend do Secure Endpoint. Distinguir partes ruidosas de aplicativos legítimos é uma etapa muito importante na manutenção de um endpoint produtivo e seguro.

A finalidade deste documento é ajudar a distinguir as operações do arquivo (criar, mover e copiar) e as execuções que terão um efeito negativo no desempenho do daemon e desperdiçarão os ciclos da CPU. A identificação desses caminhos de arquivos e diretórios permitirá que você crie e mantenha os conjuntos de exclusões apropriados para sua organização.

Você pode adicionar listas de exclusão pré-criadas às suas políticas que são mantidas pela Cisco para fornecer melhor compatibilidade entre o conector Secure Endpoint e o antivírus, a segurança ou outro software. Essas listas estão disponíveis na página Exclusões no console como Exclusões Mantidas pela Cisco.

Tipos de ajuste

Há três tipos de opções de ajuste de exclusão disponíveis:

1. **Ajuste de pré-instalação - isso pode ser feito antes da instalação do conector Mac de ponto de extremidade seguro. Ele fornecerá a você a visão mais clara de quais aplicativos e caminhos estão mais ocupados na sua máquina. No entanto, é um processo muito barulhento e exige que o usuário faça uma boa análise e agregação sozinho.**
2. **Support Tool Tuning** - isso pode ser feito depois que o conector Mac é instalado e pode ser executado em qualquer endpoint sem binários adicionais. Ele executa um olhar limitado e é excelente para identificar aplicativos problemáticos.
3. **Ajuste de Procmon** - esse processo também exige a instalação do conector, mas também exige o uso do binário Procmon, nossa ferramenta de ajuste personalizada. É essencialmente uma versão mais sofisticada do recurso de ajuste da ferramenta de suporte. Esse método exige a maior quantidade de configuração; no entanto, ele oferece os melhores resultados.

1. Ajuste pré-instalação

O ajuste pré-instalação é a forma mais básica de ajuste e é feito principalmente através da linha de comando em uma sessão de terminal.

Para mac mais recente do OS X El Capitan, você precisará primeiro inicializar para o modo de recuperação (comando-r) enquanto inicializa e desativa a proteção para dtrace:

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

Para inspecionar quais execuções de arquivos são mais predominantes, execute o seguinte procedimento:

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

Isso geralmente mostrará quais aplicativos estão sendo executados repetidamente. Muitos aplicativos de provisionamento executarão scripts ou executarão binários em curtos intervalos para manter as políticas de software da empresa. Quaisquer candidaturas que sejam vistas como executadas a uma taxa superior a uma vez por segundo, ou executadas várias vezes em surtos curtos, devem ser consideradas um bom candidato para exclusão.

Para inspecionar quais operações de arquivo são mais predominantes, execute o seguinte comando:

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

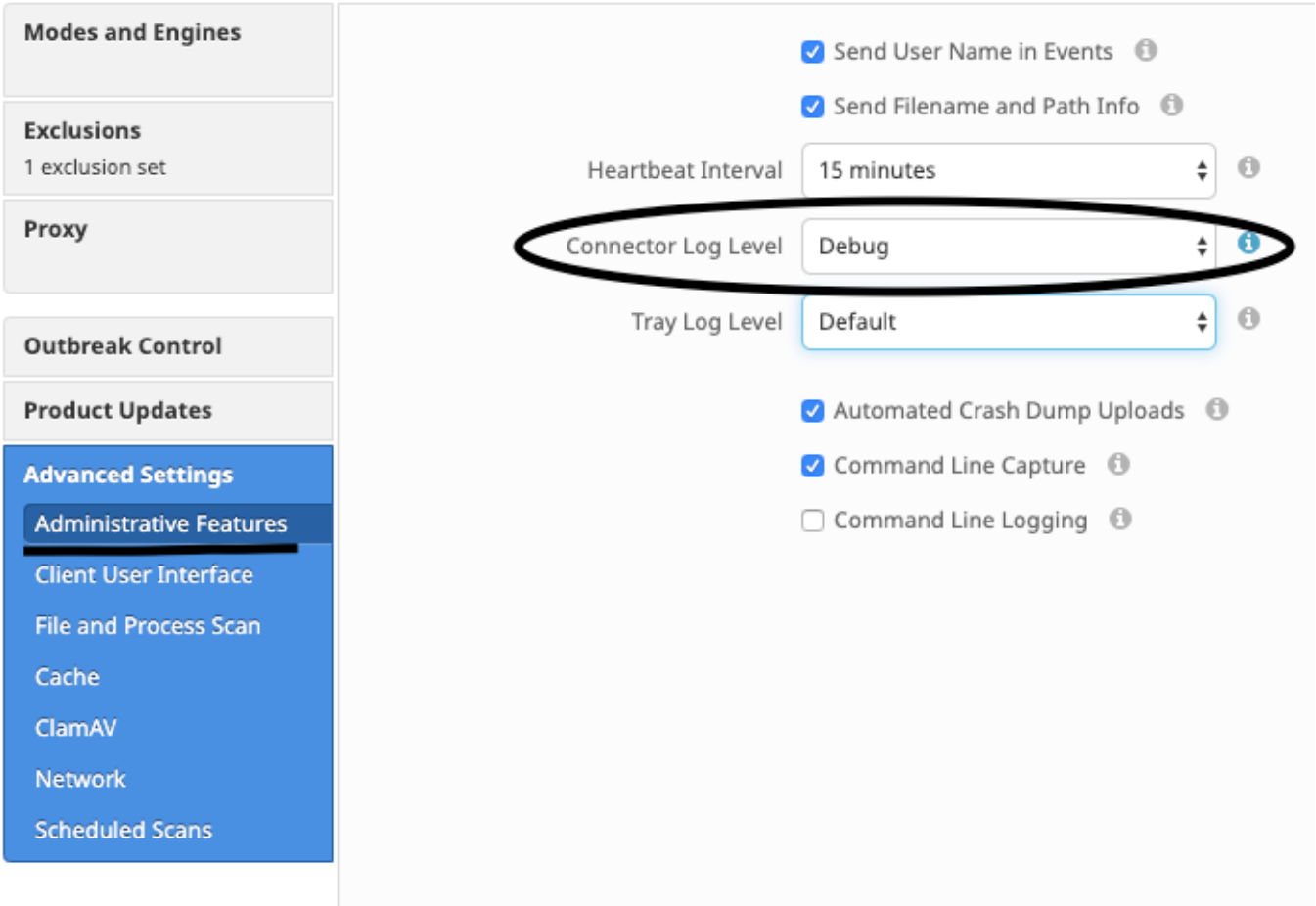
Você verá imediatamente quais arquivos estão sendo gravados na maioria. Frequentemente, esses arquivos de log serão gravados por meio da execução de aplicativos, da cópia de software

de backup ou de aplicativos de e-mail que gravam arquivos temporários. Além disso, uma boa regra é que qualquer coisa com uma extensão de arquivo de log ou diário deve ser considerada um candidato de exclusão adequado.

2. Ferramenta de suporte Ajuste

Ativando o registro de depuração

O daemon do conector precisa ser colocado no modo Debug Logging antes de iniciar o ajuste de arquivos. Isso é feito através do console Secure Endpoint, através das configurações de política do conector em *Management -> Policies*. Selecione a diretiva, Editar a diretiva e vá para a seção *Recursos administrativos* na barra lateral *Configurações avançadas*. Altere a configuração do *Nível de log do conector* para **Depurar**.



Próximo, salve sua política. Depois que sua política tiver sido salva, garantir que ele foi sincronizadohronizado para aConector. Execute o comandoconector neste modo para pelo menos 15 a 20 minutos antes de continuar com o resto do ajuste.

NOTE: Quando o ajuste estiver concluído, não esquecer alterar o *nível de log do conector* como redefinir para **Padrão** para que cconector execuções in seu mais eficientes e modo efetivo.

Executando a ferramenta de suporte

Esse método envolve o uso da Ferramenta de suporte, um aplicativo instalado com o conector Mac do Secure Endpoint. Ele pode ser acessado na pasta Aplicativos clicando duas vezes em /Applications->Cisco Secure Endpoint->Support Tool.app. Isso gerará um pacote de suporte

completo contendo arquivos de diagnóstico adicionais.

Um alternativa, e mais rápido, é executar o comando linha de comando a seguir de a Terminal sessão:

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

Isso resultará em um arquivo de suporte muito menor contendo apenas os arquivos de ajuste relevantes.

Seja como for, a Ferramenta de Suporte gerará um arquivo zip na sua Área de Trabalho que contém dois arquivos de suporte de ajuste: fileops.txt e exec.txt. fileops.txt contém uma lista dos arquivos mais frequentemente criados e modificados na sua máquina. o arquivo exec.txt conterá a lista dos arquivos executados com mais frequência. As duas listas são ordenadas pela contagem de verificações, o que significa que os caminhos verificados com mais frequência aparecem no topo da lista.

Deixe o conector em execução no modo de depuração por um período de 15 a 20 minutos e execute a ferramenta de suporte. Uma boa regra é que quaisquer arquivos ou caminhos que em média 1000 acessos ou mais durante esse período são bons candidatos a serem excluídos.

Criando exclusões de caminho, curinga, nome de arquivo e extensão de arquivo

Uma maneira de começar com as regras de Exclusão de Caminho é encontrar os caminhos de arquivos e pastas mais frequentemente verificados de fileops.txt e, em seguida, considerar a criação de regras de exclusão para esses caminhos. Depois de fazer o download da diretiva, monitore o novo uso da CPU. Pode levar de 5 a 10 minutos depois que a diretiva é atualizada antes que você perceba a queda no uso da CPU, pois pode levar tempo para que o daemon se recupere. Se ainda estiver vendo problemas, execute a ferramenta novamente para ver quais novos caminhos você observa.

- Uma boa regra é que qualquer coisa com uma extensão de arquivo de log ou diário deve ser considerada um candidato de exclusão adequado.

Criando exclusões de processos

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).
Para obter as melhores práticas sobre exclusões de processos, consulte:Endpoint seguro: Exclusões de processos em MacOS e Linux

Um bom padrão de ajuste é identificar primeiro os processos com um alto volume de execuções de exec.txt, localizar o caminho para o executável e criar uma exclusão para esse caminho. No entanto, há alguns processos que não devem ser incluídos, entre eles:

- Programas de utilitário geral - Não é recomendável excluir programas de utilitário geral (por exemplo: usr/bin/grep) sem contar o seguinte. O usuário pode determinar qual aplicativo está chamando o processo (por exemplo: localizar o processo pai que está executando grep) e excluir o processo pai. Isso deve ser feito se e somente se o processo pai puder ser transformado com segurança em uma exclusão de processo. Se a exclusão principal se aplicar a crianças, as chamadas a quaisquer filhos do processo principal também serão excluídas.O usuário que está executando o processo pode ser determinado. (ex: se um processo estiver sendo chamado em um volume alto pelo usuário "root", é possível excluir o processo, mas somente para o usuário especificado "root", isso permitirá que o Secure Endpoint monitore execuções de um determinado processo por qualquer usuário que não seja "root").**NOTA: as exclusões de processos são novas nas versões 1.11.0 e mais recentes do conector. Por causa disso, os programas de utilitário geral podem ser usados como uma exclusão de caminho no conector versão 1.10.2 e anterior. No entanto, esta prática só é recomendada quando uma compensação de desempenho é absolutamente necessária.**

Encontrar o processo pai é importante para as exclusões do processo. Depois que o processo pai e/ou o usuário do processo forem encontrados, o usuário poderá criar a exclusão para um usuário específico e aplicar a exclusão do processo aos processos filhos, o que, por sua vez, excluirá processos ruidosos que não podem ser transformados em exclusões de processos.

Identificar o processo pai

1. Do exec.txt, identifique o processo de alto volume (ex: /bin/rm).

2. Abra o arquivo ampdaemon.log do pacote de suporte, unzip syslog.tar, depois siga o caminho /Library/Logs/Cisco/ampdaemon.log (disponível apenas no pacote de suporte completo, não em um pacote de suporte gerado com as opções padrão).
3. Procure ampdaemon.log para excluir o processo. Localize a linha de log que mostra a execução do processo (ex: 19 de agosto 09:47:29 devs-Mac.local [2537] [fileop]:[info]-[kext_processor.c@938]:[210962]: Daemon Rx: NÓ:EXECUTE X:6210 P:3296 PP:3200 U:502 [/bin/rm]).
4. Identifique o processo pai usando um dos seguintes métodos: Identifique o caminho do processo pai que pode seguir o caminho do processo a ser excluído (ex: [/bin/rm] [*caminho do processo pai*]).Se o log não incluir o caminho do processo pai, identifique a ID do processo pai na seção `PP:` da linha de log (ex: PP:3200).
5. Usando o caminho pai ou a ID do processo pai, repita as etapas 3 e 4 para determinar o pai do processo pai atual. Continue esse processo até que nenhum pai possa ser determinado ou a ID do processo pai = 1 (ex: PP:1).
6. Quando a árvore de processos for conhecida, procure o caminho do programa que cobre a maioria ou todas as operações que devem ser excluídas e identifique exclusivamente o aplicativo. Isso minimiza a chance de excluir involuntariamente as operações executadas por outro aplicativo.

Identificar o usuário do processo

1. Siga as etapas de 1 a 3 de Identificação do processo pai, acima.
2. Identifique o usuário de um processo usando um dos seguintes métodos: Localize a ID de usuário do processo especificado em `U:` na linha de log (ex: U:502).Na janela Terminal, execute o seguinte comando: `dscl . list /Users UniqueID | grep #`, onde # é a ID do usuário.Você deve ver uma saída semelhante a: `Nome de usuário 502`, onde `Nome de usuário` é o Usuário do processo especificado.
3. Esse nome de usuário pode ser adicionado a uma Exclusão de processo na categoria Usuário para reduzir o escopo da exclusão, o que, para determinadas exclusões de processo, é importante. **OBSERVAÇÃO: se o usuário de um processo for o usuário local da máquina e essa exclusão tiver que se aplicar a várias máquinas com usuários locais diferentes, a categoria Usuário deverá ser deixada em branco para permitir que a Exclusão do processo se aplique a todos os usuários.**