Coleta de dados de diagnóstico do conector Linux da AMP para endpoints

Contents

[Introduction](#)
[Gerar arquivo de diagnóstico](#)
[Modo de Depuração](#)
[Usar console AMP](#)
[Ativar modo de depuração](#)
[Desativar modo de depuração](#)
[Usar linha de comando](#)
[Ativar modo de depuração](#)
[Desativar modo de depuração](#)
[Ajuste da ferramenta de suporte durante a depuração](#)
[Ajuste de exclusão](#)
[Informações Relacionadas](#)

Introduction

Este documento descreve as etapas para gerar um arquivo de diagnóstico a partir do conector Linux AMP for Endpoints. Se você tiver um problema técnico com o conector Linux, um engenheiro de suporte técnico da Cisco pode querer analisar as mensagens de registro disponíveis em um arquivo de diagnóstico.

Gerar arquivo de diagnóstico

Com o uso desse comando, você pode gerar um arquivo de diagnóstico diretamente da CLI (Command Line Interface, interface de linha de comando) do Linux:

```
/opt/cisco/amp/bin/ampsupport
```

Isso cria um arquivo .7z em sua área de trabalho. Você pode fornecer esse arquivo ao Cisco Technical Assistance Center (TAC) para análise posterior.

Modo de Depuração

O modo de depuração do Connector fornece verbosidade adicional ao registro. Ele permite mais informações sobre um problema com o conector. Esta seção descreve como ativar o modo de depuração em um conector.

> **aviso:** O modo de depuração deve ser ativado somente se a Cisco solicitar esses dados. Se você habilitar o modo de depuração por mais tempo, ele poderá preencher o espaço em disco muito rapidamente e poderá impedir que o arquivo de diagnóstico de suporte reúna o

log do conector devido ao tamanho excessivo do arquivo.

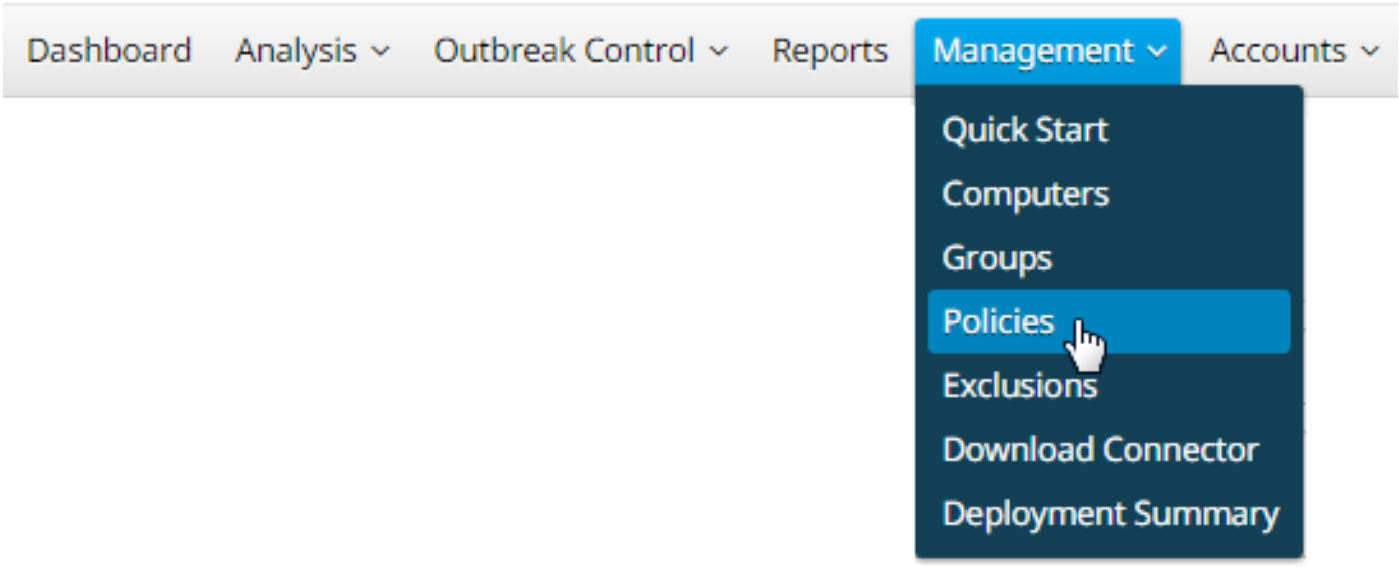
Usar console AMP

Ativar modo de depuração

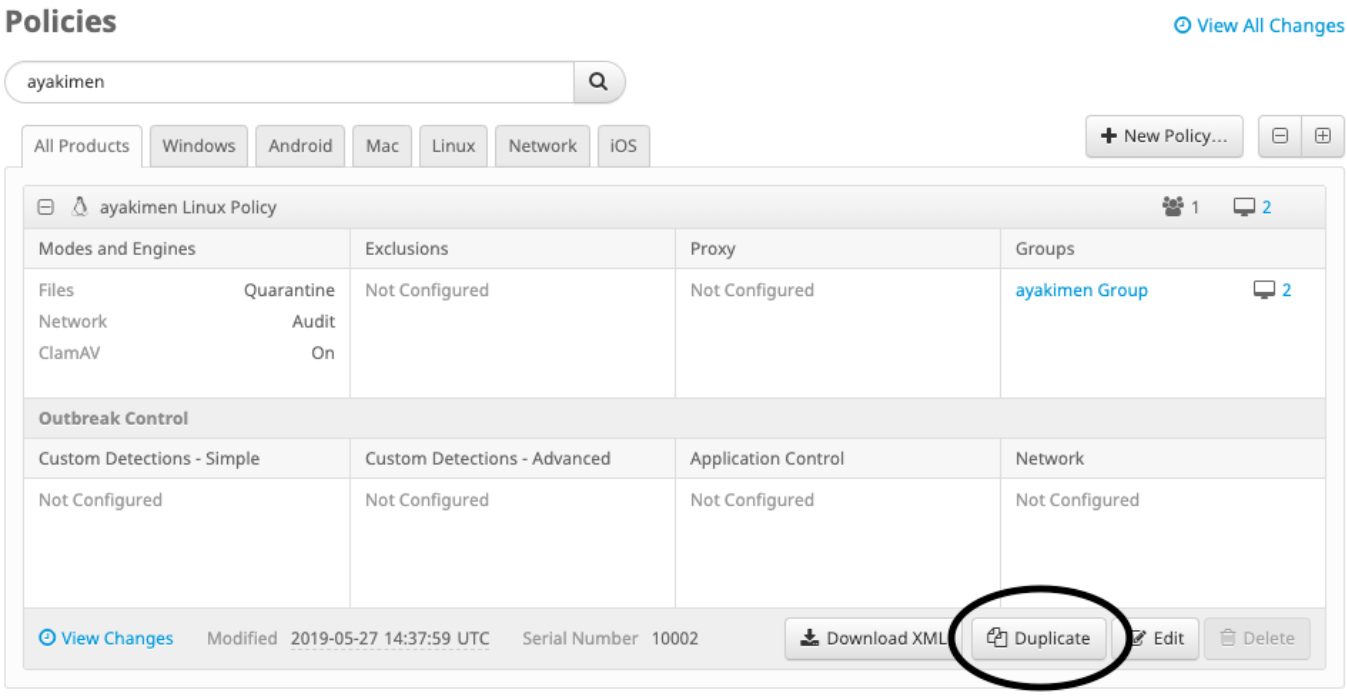
Você pode ativar o modo de depuração na política atual com as etapas 5 a 7 ou criar uma nova política no modo de depuração com todas estas etapas:

Etapa 1. Efetue login no console AMP.

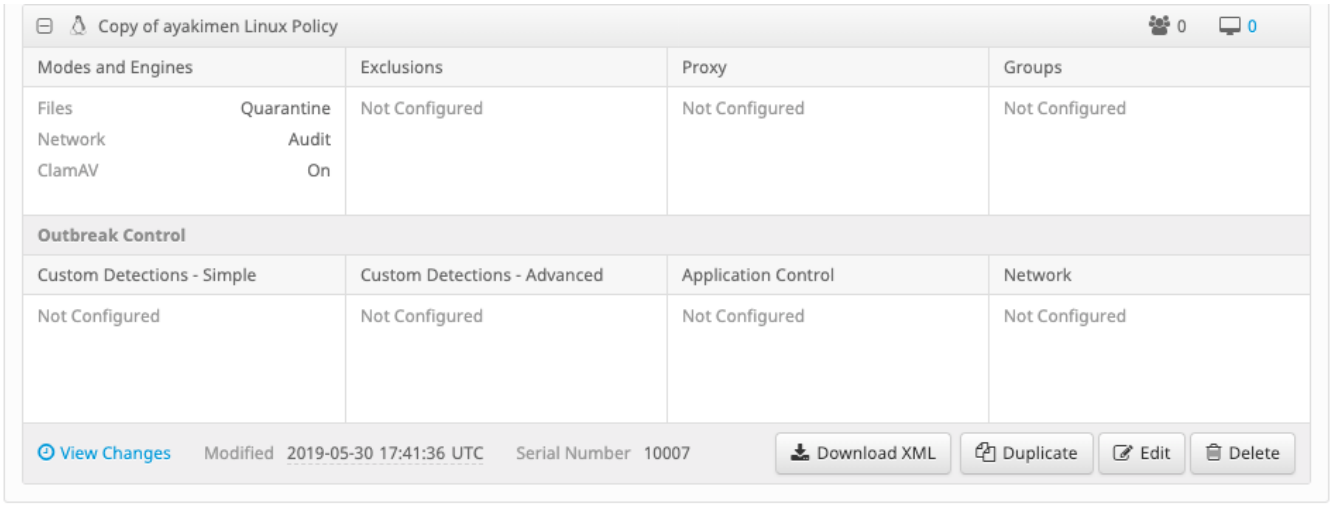
Etapa 2. Selecione **Gerenciamento > Políticas**.



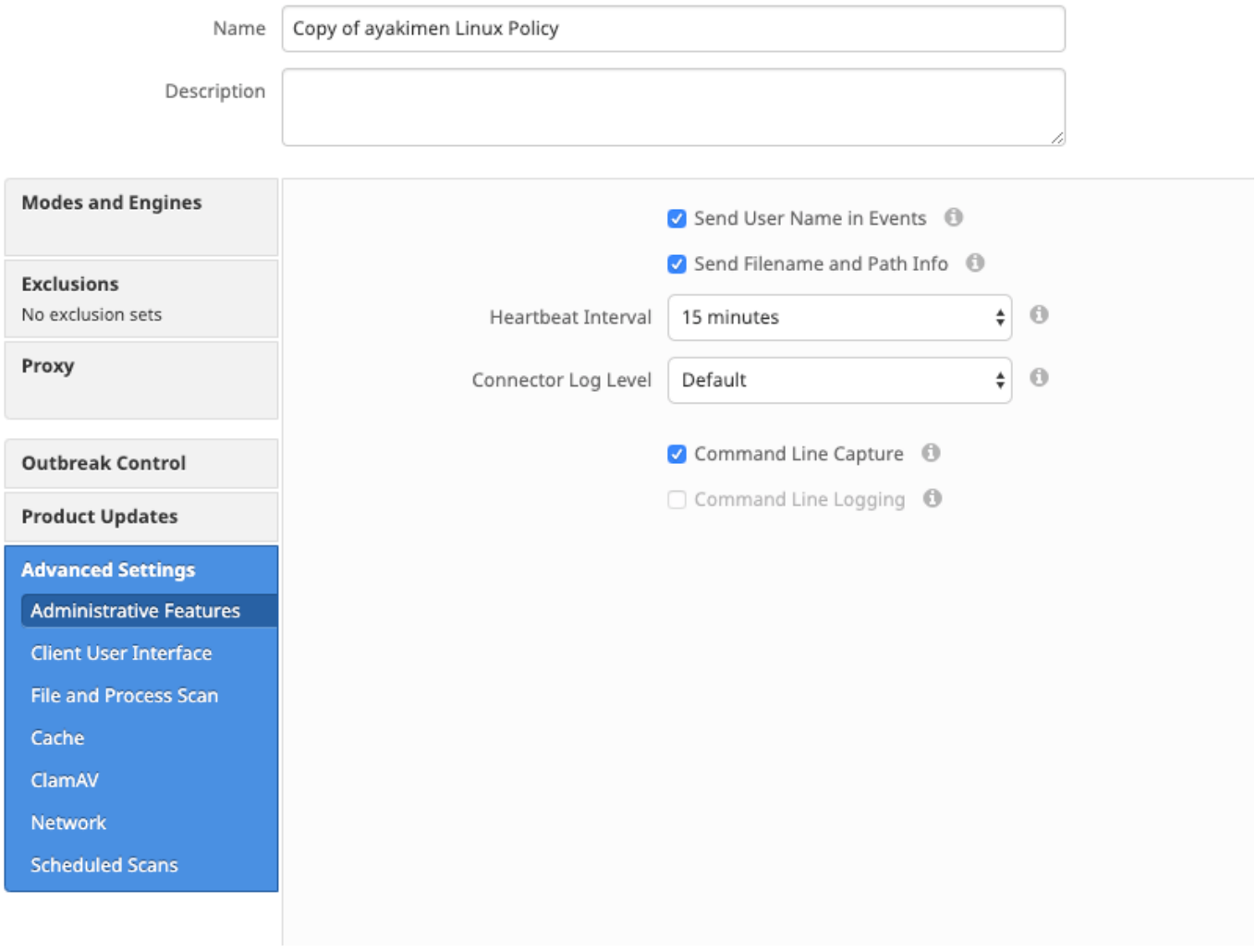
Etapa 3. Localize a Política aplicada ao dispositivo final ou computador e clique em Política. Isso expandirá a janela Política. **Clique em Duplicar**.



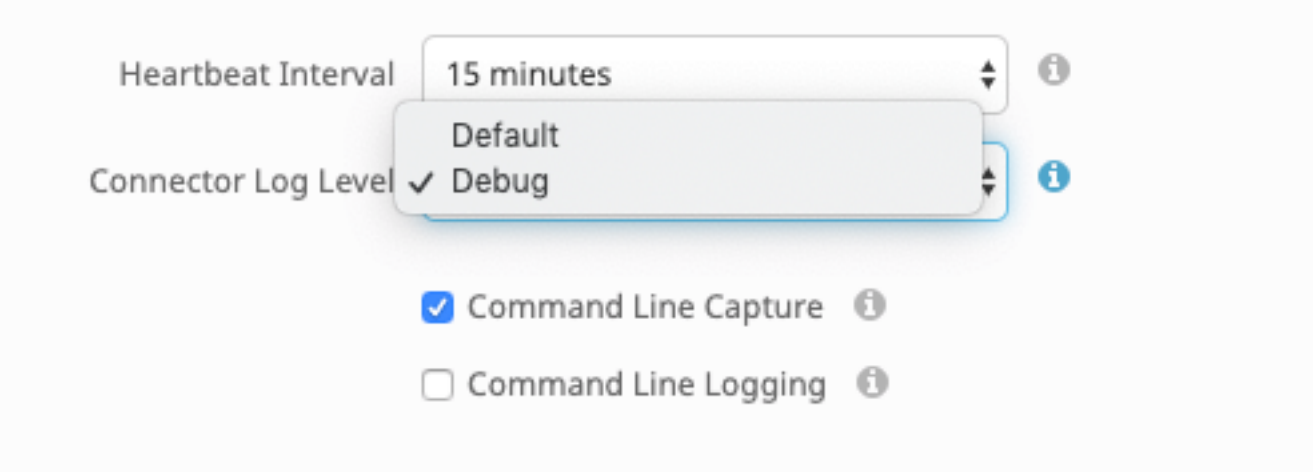
Etapa 4. Depois de **clicar em Duplicar**, o console AMP é atualizado com a política copiada.



Etapa 5. **Clique em Editar**, **clique em Configurações avançadas** e selecione **clique em** Recursos **administrativos** na barra lateral.



Etapa 6. **Para Nível de log do conector**, selecione Debugnas listas suspensas.



Passo 7. Clique em Salvar para salvar as alterações.

Etapa 8. Depois de salvar a nova política, você precisa criar/alterar um grupo para incluir *a nova política* e *o* dispositivo *final* onde deseja gerar informações de depuração.

Desativar modo de depuração

Para desabilitar o modo de depuração, siga as mesmas etapas que você concluiu para habilitar o modo de depuração, mas altere o **Nível de log do conector** para **Padrão**.

Usar linha de comando

Ativar modo de depuração

Se você tiver problemas de conectividade com o console e quiser ativar o modo de depuração, execute estes comandos na CLI:

```
/opt/cisco/amp/bin/ampcli
ampcli>debuglevel 1
```

Esta é a saída:

```
ampcli>debuglevel 1
Daemon now logging at 'info' level until next policy update
```

Desativar modo de depuração

Para desativar o modo de depuração, use estes comandos:

```
/opt/cisco/amp/bin/ampcli
ampcli>debuglevel 0 Daemon now logging at 'notice' level until next policy update
```

Ferramenta de suporte Ajustando durante a depuração

O daemon do Connector precisa ser colocado no modo Debug Logging antes de iniciar o ajuste de arquivos. Isso é feito através do console AMP, através das configurações de política do conector *em Gerenciamento -> Políticas*. Edite a diretiva e vá para *a* seção Recursos

Administrativos na guia Configurações *avançadas*. Altere *a* configuração do nível de *log do conector* para Depurar.

Em seguida, salve sua política. Depois de salvar a política, verifique se ela foi sincronizada com o conector. Execute o conector neste modo por pelo menos 15 a 20 minutos antes de continuar com o resto do ajuste.

Nota: Quando o ajuste estiver concluído, não se esqueça de alterar *a* configuração *do* nível de registro do conector para Defaultado para que o conector seja executado no modo mais eficiente e eficaz.

Executando a ferramenta de suporte

Esse método envolve o uso da ferramenta de suporte, um aplicativo instalado com o conector AMP Mac. Ele pode ser acessado na pasta Aplicativos clicando duas vezes em /Applications->Cisco AMP->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 seguirde a Terminal sessão:

```
sudo /opt/cisco/amp/bin/ampsupport -x
```

```
sudo /opt/cisco/amp/bin/ampsupport
```

A primeira opção resultará em um arquivo de suporte muito menor contendo somente os arquivos de ajuste relevantes. A segunda opção fornece um pacote de suporte completo que contém mais informações, como registros, que podem ser necessários para ajustar exclusões de processos (disponíveis no Connector versões 1.11.0 e mais recentes).

Seja como for, a Ferramenta de Suporte gerará um arquivo zip em sua ~casa que contém dois arquivos de suporte de ajuste: fileops.txt e exec.txt. fileops.txt contém uma lista dos arquivos criados e modificados com mais frequência na sua máquina, que serão úteis para exclusões de caminho/curinga. o arquivo exec.txt conterá a lista dos arquivos executados com mais frequência, que serão úteis para Exclusões de Processo. 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.

Ajuste de exclusão

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 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 Linux can only be implemented for ELF files. Users cannot implement Process Exclusions for file formats such as .sh (Shell Scripts).
Para obter as melhores práticas sobre exclusões de processos, consulte: AMP para endpoints: 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 AMP monitore execuções de um determinado processo por qualquer usuário que não seja "root").**OBSERVAÇÃO: as exclusões de processos são novas no Connector versões 1.11.0 e mais recentes. Por causa disso, os programas de utilitário geral podem ser usados como uma exclusão de caminho nas versões 1.10.2 e mais antigas do Connector. 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. 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:0).Na janela Terminal, execute o seguinte comando: `getent passwd # | cut-d: -f1`, onde # é a ID do usuário.Você deve ver uma saída semelhante a: `Nome de usuário`, onde Nome de usuário é o usuário do processo especificado.
3. Este O nome de usuário pode ser adicionado a uma Exclusão de processo na categoria Usuário para reduzir o escopo da exclusão, o que, para certas 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.**

Informações Relacionadas

- Coleta de dados de diagnóstico de um conector FireAMP em execução no Windows
- Coleta de dados de diagnóstico de um conector FireAMP em execução no Mac OS
- Suporte Técnico e Documentação - Cisco Systems