Guia básico de solução de problemas para o conector Linux da AMP para endpoints

Contents

Introduction

Este documento descreve uma maneira básica de solucionar problemas de desempenho ligado o Cisco Advanced Malware Protection (AMP) para Conector Linux de endpoints.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- AMP para endpoints
- Linux/UnixSistemas operacionais baseados em

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Red Hat Enterprise Linux (RHEL) / Sistema Operacional Corporativo Da Comunidade (ClienteSO) versões 6.10 e 7.7
- AMP para Endpoints Linux Conector versão 1.11.1

Para obter uma lista completa das versões compatíveis da AMP com o sistema operacional Linux, consulte este artigo.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O conector da AMP verifica todos os arquivos ativos (aqueles que se movem, copiam e/ou modificam) em uma máquina, a menos que explicitamente indicado, isso inevitavelmente traz problemas de desempenho se muitos processos e operações forem executados enquanto o conector está ativo, o que leva a uma alta utilização da CPU, a uma lentidão e, em alguns casos, a um software que não será executado ou executado lentamente. Além disso, o conector AMP pode bloquear arquivos com base na reputação da nuvem, o que pode, em alguns momentos, ser errado (falso positivo). A solução para ambos os problemas é excluir Estes caminhos e processos; no caso de problemas falsos positivos, não relacionados ao desempenho ou problemas de desempenho que não pareçam ser resolvidos por meio deste guia, é recomendável aumentar o suporte de tíquetes.

O fluxo de solução de problemas básicos de desempenho é o seguinte:

- Colete um pacote de depuração enquanto o problema é reproduzido.
- Execute a ferramenta de suporte AMP
- Revisar os arquivos pertinentes
- Adicionar exclusões conforme necessário

Troubleshoot

Como coletar um pacote de depuração

Um pacote de depuração é um arquivo zip que contém informações de depuração detalhadas (como logs de varredura) no conector. Esse pacote é essencial para solucionar a maioria dos problemas relacionados ao conector do AMP para endpoints. Para coletar um pacote de depuração, siga as etapas fornecidas na Coleta de Dados de Diagnóstico do AMP para Endpoints Linux Connector.

Que informações a ferramenta de suporte do amp coleta e, em seguida, um pacote de depuração é executado?

A entrada do processo do pacote de depuração mostra que o comando *o ampsupport executa alguns comandos de coleta de log, como mostrado na imagem.*

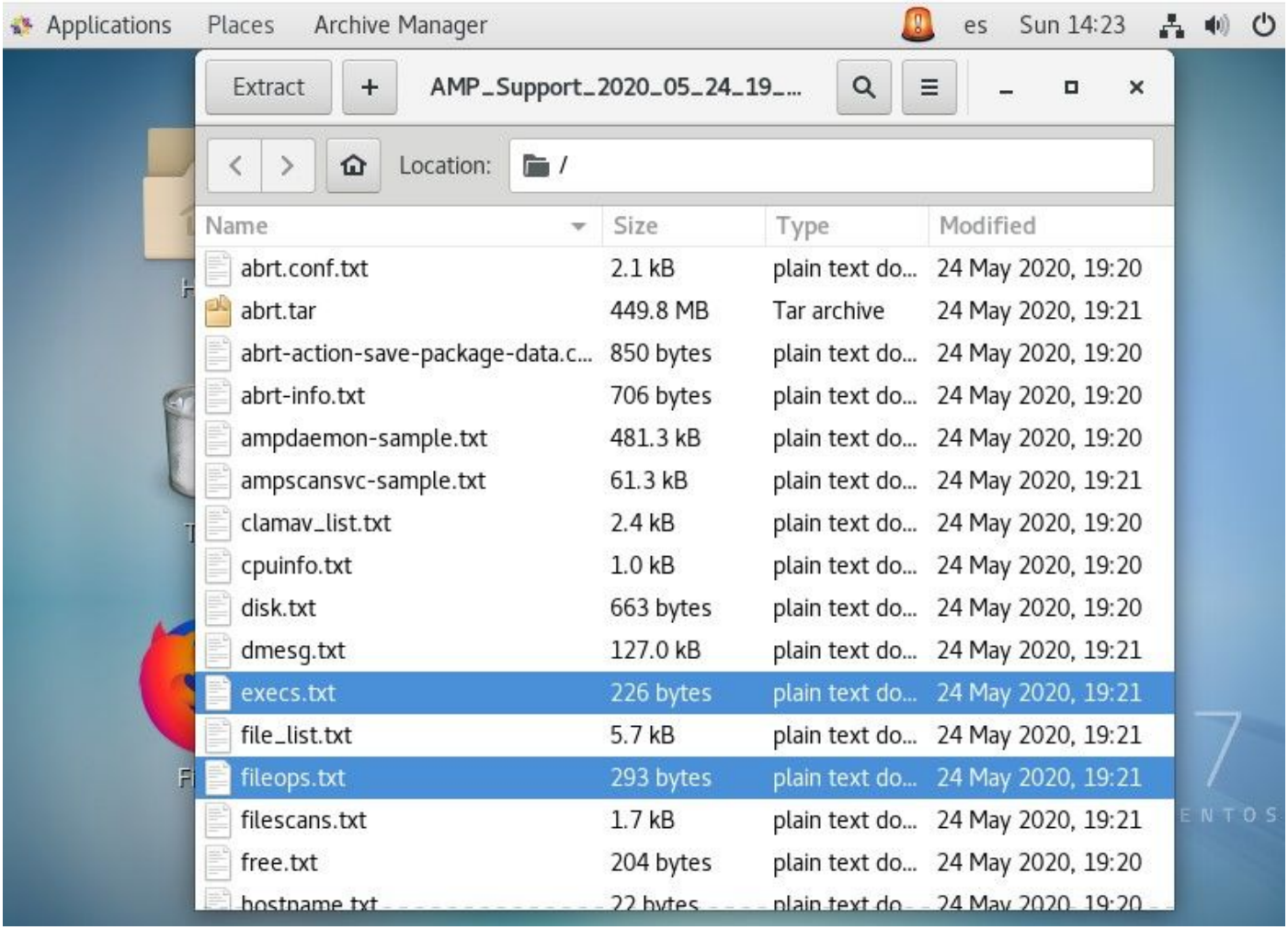
```
top -b -n5 -d2 -H -p `pidof ampdaemon | tr ' ' ,` -p `pidof ampscansvc | tr ' ' ,`
[ -e 'abrt-cli' ] && abrt-cli list -d
[ -d '/var/spool/abrt' ] && for dir in $(find /var/spool/abrt/*/ -type d -maxdepth 1);
do echo -e "
Crash: ${dir}"; echo -e "
Kernel: $(cat "${dir}/kernel")"; echo -e "
Count: $(cat "${dir}/count")";echo -e "
Executable: $(cat "${dir}/executable")"; echo -e "
Uid: $(cat "${dir}/uid")";echo -e "
Reason: $(cat "${dir}/reason")"; echo -e "
Package: $(cat "${dir}/package")"; done
find: warning: you have specified the -maxdepth option after a non-option argument -typ
e, but options are not positional (-maxdepth affects tests specified before it as well
as those specified after it).  Please specify options before other arguments.

cat: /var/spool/abrt/oops-2020-05-18-18:21:09-10472-0//executable: No such file or dire
ctory
[ -e '/etc/abrt/abrt.conf' ] && cat '/etc/abrt/abrt.conf'
[ -e '/etc/abrt/abrt-action-save-package-data.conf' ] && cat '/etc/abrt/abrt-action-sav
e-package-data.conf'
cat /proc/slabinfo
```

Como ler os registros básicos do pacote Linux para identificar os caminhos e

processos afetados

O pacote Linux AMP for Endpoints Debug transporta a plethora de informações úteis, no entanto, para fins básicos de solução de problemas de desempenho, há apenas alguns arquivos a serem revisados, fileops.txt, fiescans.txt e exec.txt, como mostrado na imagem.



O arquivo de texto Operações de arquivos (fileops) funciona como a principal ferramenta de solução de problemas de desempenho. ele lista todas as operações atualmente ativas em seu endpoint enquanto o conector é executado. Esses são os caminhos a serem adicionados ao conjunto de exclusão da política, se for considerado necessário/seguro.

O texto é o seguinte:

- <Varredura de números realizada no caminho executado enquanto o processo de coleta de pacotes é executado> /<Caminho digitalizado>

Exemplo de varredura:

- 1 /homet/user/.mozila/Firefox/

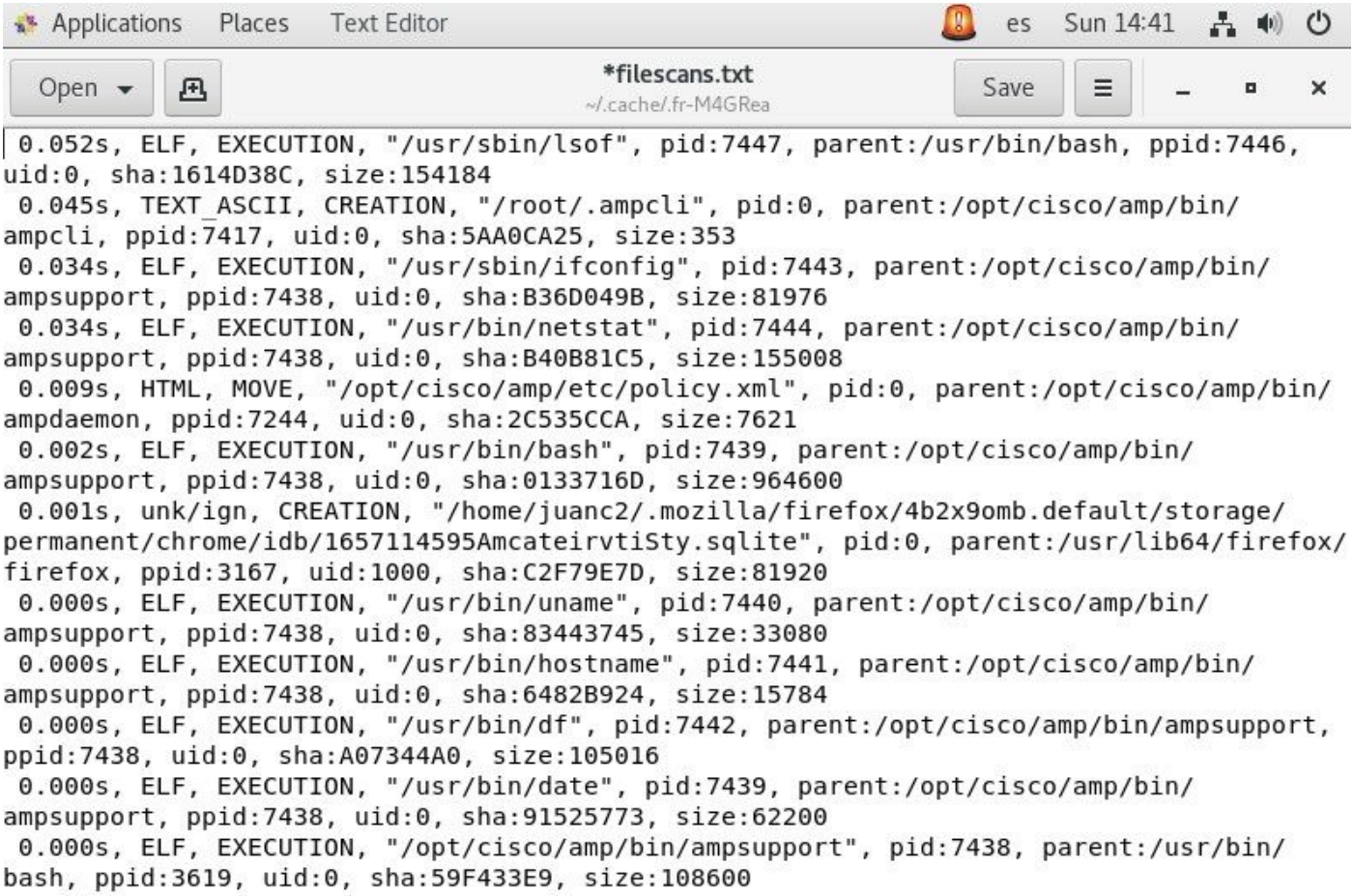
O arquivo de texto de verificação de arquivo (arquivos) lista todos os processos executados enquanto o conector coletou informações de depuração.

O texto é o seguinte:

- <Tempo de execução> , <Tipo de arquivo>, <Tipo de operação>, <Caminho do processo pai>, <ID do processo pai>, <ID do processo pai>, <Assinatura SHA (não SHA256)> <Tamanho do arquivo>

O arquivo de texto Execução de Arquivos (exec) lista todos os comandos Linux usados por processos ativos no conector enquanto o conector coletou o pacote.

> **Aviso**: Os caminhos listados aqui não devem ser excluídos na política de AMP, pois são binários (/bin) e binários de sistema (/sbin) que todo processo utiliza, entretanto, essa lista pode ser útil para tentar entender quais ações são executadas pelos diferentes processos executados na máquina de destino.



Depois de identificado, o caminho deve ser excluído por meio de políticas. Siga as Melhores formas de aprendizado da AMP para exclusões de endpoints.

As exclusões de processos tratadas pelos conectores Mac e Linux são adicionadas de forma semelhante através da política, no entanto, o método difere ligeiramente: Exclusões de processos em macOS e Linux.

Depois que as exclusões forem adicionadas, teste e monitore se o problema persistir. Entre em contato com o Suporte TAC da AMP.