Solucionar Falhas do Conector do Secure Endpoint Linux

Contents

Introdução

Este documento descreve as falhas que o conector do Cisco Secure Endpoint Linux usa para notificá-lo sobre as condições que afetam seu funcionamento adequado.

Informações de Apoio

O conector Cisco Secure Endpoint Linux notifica com um evento Fault Raised quando detecta uma condição que afeta o funcionamento adequado do conector. Da mesma forma, um evento Fault Cleared comunica que a condição não está mais presente.

Tabela de Falhas do Conector Linux de Ponto de Extremidade Seguro

A tabela descreve as falhas e as etapas de diagnóstico associadas.

ID da falha	Descrição	Solução de problemas/resolução
5	Usuário do serviço de varredura indisponível	O conector não conseguiu criar um usuário para executar o processo de varredura de arquivos. O conector usa o usuário raiz para executar verificações de arquivos como uma solução alternativa. Isso se desvia do projeto pretendido e não é esperado. Se a `cisco-amp-scan-svc` o usuário ou grupo foi excluído ou a configuração do usuário e do grupo foi alterada; em seguida, você pode reinstalar o conector para recriar o usuário e o grupo com as configurações necessárias. Detalhes adicionais estão disponíveis em */var/log/cisco/ampdaemon.log*. Se a criação do grupo de usuários for restrita por meio das configurações em **/etc/login.defs** esse arquivo deverá ser temporariamente alterado enquanto o instalador estiver em execução para permitir que o usuário e o grupo sejam criados. Para fazer isso, altere **usergroups_enab** de não para sim. Essa falha pode ser gerada nos conectores Linux 1.15.1 e mais recentes se

		outro programa tiver modificado uma das permissões de diretório do conector (ou seja, /opt/cisco ou um diretório filho). Para aliviar isso, a permissão de diretório alterada deve ser redefinida para o padrão (ou seja, 0755), garantir que nenhum programa futuro modifique o diretório /opt/cisco (ou qualquer diretório filho) e reinicie o serviço de conector.
6	Verificar o serviço reiniciando com frequência	O processo de verificação de arquivo do conector encontrou falhas repetidas e o conector foi reiniciado em uma tentativa de limpar a falha. É possível que um ou mais arquivos no sistema causem falha no algoritmo de verificação quando examinados. O conector continua com as varreduras na base de melhor esforço. Se essa falha não for automaticamente eliminada em 10 minutos após o início do conector, isso é uma indicação de que é necessária uma intervenção adicional do usuário e a capacidade do conector de executar varreduras é prejudicada. Consulte */var/log/cisco/ampdaemon.log* e */var/log/cisco/ampscansvc.log* para obter detalhes.
7	Falha ao iniciar o serviço de verificação	O processo de varredura de arquivos do conector não pôde ser iniciado e o conector foi reiniciado na tentativa de eliminar a falha. A funcionalidade de verificação de arquivo está desabilitada enquanto essa falha é gerada. Essa falha poderá ser disparada se for encontrado um erro ao carregar arquivos de definição de vírus (arquivos .cvd) recém-instalados. O conector executa várias verificações de integridade e estabilidade antes de ativar novos arquivos .cvd para evitar essa falha. Ao reiniciar, o conector remove todos os arquivos .cvd inválidos para que o conector possa continuar. Se essa falha não for eliminada quando o conector for reiniciado, isso é uma indicação de que é necessária uma intervenção adicional do usuário. Se essa falha se repetir a cada atualização .cvd, isso é uma indicação de que um arquivo .cvd inválido não está sendo detectado corretamente pelas verificações de integridade do arquivo .cvd do conector. Essa falha poderá ser disparada nos conectores Linux se a máquina estiver com pouca memória disponível e o serviço de scanner não puder ser iniciado. Consulte o "Guia do usuário do Secure Endpoint (anteriormente AMP para endpoints)" para obter os requisitos mínimos do sistema para Linux. Consulte */var/log/cisco/ampdaemon.log* e */var/log/cisco/ampscansvc.log* para obter detalhes.
8	Falha ao iniciar o monitor do sistema de arquivos em tempo real	â€‹O módulo do kernel que fornece o monitoramento de atividade do sistema de arquivos em tempo real não foi carregado e a política do conector tem a opção "Monitorar cópias e movimentações de arquivos" habilitada. Essas funções de monitoração não estão disponíveis no conector enquanto essa falha é gerada. Essa falha é gerada quando o

		conector de Ponto de Extremidade Seguro não pode carregar o módulo de kernel subjacente necessário para o monitoramento da atividade do sistema de arquivos. A Inicialização Segura da UEFI deve estar desabilitada no sistema. Se a Inicialização Segura estiver desativada, essa falha pode ser causada por uma incompatibilidade entre o módulo de kernel ampavflt ou ampfsm fornecido com o conector de Ponto Final Seguro e o kernel do sistema ou outros módulos de kernel de terceiros instalados no sistema. Revise */var/log/messages* para obter detalhes ou desabilite o monitoramento de arquivos nas configurações de política do conector para eliminar essa falha. A falha também pode ser causada durante a execução de uma versão do kernel que não é suportada pelo conector. Neste caso, pode ser limpo construindo um módulo de kernel ampfsm personalizado para o kernel atual do sistema em execução. (Aplicável ao conector Linux versões 1.16.0 e mais recente.) Para obter mais informações sobre a criação de módulos de kernel personalizados, consulte: Building Cisco Secure Endpoint Linux Connector Kernel Modules
9	Falha ao iniciar o monitor de rede em tempo real	O módulo do kernel que fornece o monitoramento de atividade de rede em tempo real não foi carregado e a política do conector tem a opção "Enable Device Flow Correlation" habilitada. Esta função de monitoramento não está disponível no conector enquanto esta falha é gerada. Essa falha é gerada quando o conector de Ponto de Extremidade Seguro não pode carregar o módulo de kernel subjacente necessário para o monitoramento da atividade do sistema de arquivos. A Inicialização Segura da UEFI deve estar desabilitada no sistema. Se a Inicialização Segura estiver desativada, essa falha pode ser causada por uma incompatibilidade entre o módulo de kernel ampavflt ou ampfsm fornecido com o conector de Ponto Final Seguro e o kernel do sistema ou outros módulos de kernel de terceiros instalados no sistema. Revise */var/log/messages* para obter detalhes ou desabilite o monitoramento de arquivos nas configurações de política do conector para eliminar essa falha. A falha também pode ser causada durante a execução de uma versão do kernel que não é suportada pelo conector. Neste caso, pode ser limpo construindo um módulo de kernel ampfsm personalizado para o kernel atual do sistema em execução. (Aplicável ao conector Linux versões 1.16.0 e mais recente.) Para obter mais informações sobre a criação de módulos de kernel personalizados, consulte: Building Cisco Secure Endpoint Linux Connector Kernel Modules
11	O pacote kernel-devel necessário está ausente	Para distribuições baseadas em Red Hat, o pacote em nível de kernel necessário para o sistema de arquivos em tempo real e o monitoramento de atividade de rede está ausente e a política de conector tem "Monitorar cópias e movimentações de arquivos" ou "Ativar correlação de fluxo de

		dispositivo" habilitado. Essa falha é gerada quando o conector do Secure Endpoint não consegue compilar e carregar o módulo subjacente eBPF necessário para o monitoramento da atividade do sistema de arquivos. Instale o pacote kernel-devel para o kernel em execução no momento e reinicie o conector, ou desabilite esses recursos na política para eliminar essa falha. (Aplicável somente às versões 1.13.0 e mais recentes do conector Linux.) Para Oracle Linux UEK 6 e mais recente, o pacote kernel-uek-devel é necessário para esses recursos. Instale o pacote kernel-uek-devel para o kernel em execução no momento e reinicie o conector, ou desabilite esses recursos na política para eliminar essa falha. (Aplicável somente a conectores Linux versões 1.18.0 e mais recentes.) Para distribuições baseadas em Debian, o pacote linux-headers é necessário para estes recursos. Instale o pacote linux-headers para o kernel em execução no momento e reinicie o conector, ou desabilite esses recursos na política para eliminar essa falha. (Aplicável ao conector Linux versões 1.15.0 e mais recente.) Para obter mais informações, consulte: Falha no nível de kernel do Linux
16	Kernel incompatível	O kernel em execução no momento não é compatível com o conector em execução no momento e a política de conector tem "Monitorar cópias e movimentações de arquivos" ou "Habilitar correlação de fluxo de dispositivo" habilitado. Faça o downgrade do kernel para uma versão compatível ou atualize o conector para uma versão mais recente que ofereça suporte a esse kernel. Para obter detalhes sobre as versões de kernel suportadas, consulte: Compatibilidade de SO do Cisco Secure Endpoint Linux Connector
18	O monitoramento de eventos do conector está sobrecarregado	Essa falha ocorre quando o conector está sob carga pesada devido a um número excessivo de eventos do sistema. A proteção do sistema é limitada e o conector monitora um conjunto menor de eventos críticos do sistema até que a atividade geral do sistema seja reduzida. Essa falha pode ser uma indicação de atividade mal-intencionada do sistema ou de aplicativos muito ativos no sistema. Se um aplicativo ativo for benigno e confiável para o usuário, ele poderá ser adicionado a um conjunto de exclusão de processo para reduzir a carga de monitoramento no conector. Essa ação pode ser suficiente para eliminar a falha. Se nenhum processo benigno causar carga pesada, será necessário investigar se o aumento da atividade é devido a um processo mal-intencionado.

		Se o conector estiver sob períodos curtos de carga pesada, é possível que essa falha possa se eliminar por si só. Se essa falha é gerada com frequência, não há processos benignos que causam carga pesada e nenhum processo mal-intencionado foi descoberto, então o sistema precisa ser reprovisionado para lidar com cargas mais pesadas.
19	A política do SELinux está ausente ou desabilitada	Essa falha é gerada quando a Política do Secure Enterprise Linux (SELinux) no sistema impede que o Conector monitore a atividade do sistema. Se o SELinux estiver habilitado e no modo de imposição, o Conector exigirá esta regra na Política do SELinux: `allow unconfined_service_t self:bpf { map_create map_read map_write prog_load prog_run };` Em sistemas baseados em Red Hat, incluindo RHEL 7 e Oracle Linux 7, essa regra não está presente na política padrão do SELinux. Durante uma instalação ou atualização, o Conector tenta adicionar essa regra por meio da instalação de um módulo de política SELinux chamado `cisco-secure-bpf`. Se `cisco-secure-bpf` falha ao instalar e carregar, ou está desativado, a falha é gerada. Para resolver a falha, reinstale ou atualize o Conector para disparar a instalação do cisco-secure-bpf, ou adicione manualmente a regra à Política SELinux existente e reinicie o Conector. Para obter instruções mais detalhadas sobre como modificar a política do SELinux para resolver esta falha, consulte Falha na política do SELinux.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.