Falhas do Cisco Secure Endpoint Mac Connector

Contents

Introduction

O conector pode notificá-lo de um evento de elevação de falhas quando detecta uma condição que afeta o funcionamento correto do conector. Da mesma forma, um evento Falha Limpa comunica que a condição não está mais presente.

Tabela de falhas do conector

A tabela a seguir descreve as falhas e as etapas de diagnóstico correspondentes.

ID de falha	Texto do portal	Endpoint Descrição	Solução de problemas/resolução
1	Módulo Kernel não autorizado	Extensão do sistema não autorizada	A extensão do sistema do Conector foi bloqueada. Abra as Preferências do sistema de segurança e privacidade e aprove o rama Como alternativa, as extensões do sistema podem ser aprovadas remotament usando um perfil de gerenciamento de dispositivos móveis (MDM).
2	Incompatibilidade de versão	Incompatibilidade de versão de extensão de sistema	O software Connector instalado está corrompido. Reinstale o conector. Observação: ao executar o Mac Connector versões 1.14.0 e posteriores, algu ocorrências dessa falha podem ser eliminadas ao reiniciar o computador.
3	Acesso ao disco não concedido	Acesso total ao disco não concedido	O conector não pode acessar arquivos de usuário para verificação. Abra as preferências do sistema de segurança e privacidade e conceda acesso total a disco ao serviço AMP. Para versões do Mac Connector anteriores à 1.14.0, esse processo é chamad */opt/cisco/amp/ampdaemon*. Para o Mac Connector versões 1.14.0 e posteriores, os dois aplicativos a segu requerem acesso total ao disco, dependendo da versão macOS: • *AMP para endpoints Serviço* (necessário para todas as versões macOS) • *Extensão de segurança AMP* (necessário no macOS 10.15.5 e mais rece Para o Mac Connector versões 1.14.1 e posteriores, os dois aplicativos a segu requerem acesso total ao disco, dependendo da versão macOS: • *AMP para endpoints Serviço* (necessário para todas as versões macOS) • *Extensão de segurança AMP* (necessário no macOS 11 e mais recente) Detalhes adicionais estão disponíveis nesta nota técnica.
4	Módulo	Não foi possível	Para versões do Mac Connector anteriores à 1.14.0, ou quando executado em macOS 10.14 ou 10.15, essa falha indica que a extensão do sistema do Conn

	Kernel não carregado	carregar a extensão do sistema; reinstale o conector	é a versão correta e foi aprovada para execução, mas ainda não foi carregada Consulte */Library/Logs/Cisco/ampdaemon.log* para obter detalhes. A desinstal e reinstalação do conector também pode limpar essa falha.
5	Usuário do serviço de verificação indisponível	Usuário do serviço de verificação indisponível	O conector não conseguiu criar um utilizador para executar o processo de aná de ficheiros. O conector funciona com isso usando o usuário raiz para executa verificação de arquivos. Isso se afasta do projeto pretendido e não é esperado Se a `Cisco-amp-scan-svc` usuário ou grupo excluído, ou a configuração do usuá do grupo foi alterada, reinstalar o conector recriará o usuário e o grupo com a configuração necessária. Mais detalhes estão disponíveis em */Library/Logs/Cisco/ampdaemon.log*.
6	Verificar a reinicialização do serviço com frequência	Verificar a reinicialização do serviço com frequência	O processo de verificação de arquivos do Conector encontrou falhas repetidas Conector foi reiniciado na tentativa de limpar a falha. É possível que um ou ma arquivos no sistema estejam causando o travamento do algoritmo de verificaç quando digitalizado. O conector continua com as varreduras com base no mel esforço. Se essa falha não for automaticamente eliminada dentro de 10 minutos após o início do conector, então esta é uma indicação de que é necessária mais intervenção do usuário e a capacidade do conector de realizar verificações se prejudicada. Revisão */Library/Logs/Cisco/ampdaemon.log* e */Library/Logs/Cisco/ampscans* para obter detalhes.
7	Falha ao iniciar o serviço de pesquisa	Falha ao iniciar o serviço de pesquisa	O processo de verificação de arquivos do Connector não pôde ser iniciado e o conector foi reiniciado na tentativa de limpar a falha. A funcionalidade de análi ficheiros está desativada enquanto esta falha é elevada. Essa falha pode ser disparada se um erro for encontrado ao carregar arquivos definição de vírus recém-instalados (arquivos .cvd). O conector executa várias verificações de integridade e estabilidade antes de ativar novos arquivos .cvd evitar essa falha. Após o reinício, o conector removerá 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 mais intervenção do usuário. Se essa falha se repetir com cada atualização .cvd, isso é uma indicação de que um arquivo .cv inválido não está sendo detectado corretamente pelas verificações de integrid do arquivo .cvd do conector. Revisão */Library/Logs/Cisco/ampdaemon.log* e */Library/Logs/Cisco/ampscans* para obter detalhes.
10	Reinicialização necessária para carregar o módul	Reinicialização necessária para carregar as extensões do sistema	Reinicialize o sistema. Para o conector Mac versões 1.1.1 e 1.14.0, essa falha pode ser aumentada s extensões do sistema não puderem ser carregadas. Nesse caso, essa falha p ser eliminada reinstalando o conector. Observe que o Mac Connector 1.14.1 e posterior pode gerar essa falha se hou muitas extensões de sistema do Network Content Filter instaladas no sistema. Consulte a guia de falha 13 abaixo para obter detalhes adicionais se a reinicialização do computador não apagar essa falha.

	o do kernel ou a extensão do sistema		
12	Filtro de rede não permitido	Filtro de rede não permitido	O filtro de rede é exigido pelo recurso "Habilitar correlação de fluxo de dispositivo" na política. Para limpar essa falha, permita que o 'AMP for Endpoints Service' monitore o conteúdo da rede no endpoint. A caixa de diálogo macOS para permitir o Filtro de Rede pode ser acessada clicando na falha ativa listada no menu Agente e seguindo as orientações fornecidas. Detalhes adicionais, incluindo configurações de perfil MDM para autorização remota de filtros de rede, estão disponíveis em esta nota técnica.
13	Excesso de extensões de sistema de filtro de conteúdo de rede	Excesso de extensões de sistema de filtro de conteúdo de rede	Para o Mac Connector 1.14.0, essa falha é frequentemente levantada devido a um bug macOS ao iniciar a extensão do sistema do filtro de conteúdo de rede. A reinicialização do computador limpará essa falha. O recurso "Habilitar correlação de fluxo de dispositivo" na política requer o uso de um filtro de conteúdo de rede macOS de nível de firewall. MacOS limita o número de filtros de conteúdo de rede que podem ser executados. Se essa falha for gerada e não for eliminada, reinicie o computador, desinstale os filtros de conteúdo de rede de nível de firewall que não são mais necessários e reinicie o conector.
14	Excesso de extensões de sistema de segurança de endpoint	Excesso de extensões de sistema de segurança de endpoint	O MacOS limita o número de extensões de sistema de segurança de endpoint que podem ser executadas. O conector Mac requer uma destas extensões de sistema de segurança de endpoint para os recursos 'Monitorar cópias e movimentos de arquivos' e 'Monitorar execução de processos' na política . Para limpar essa falha, desinstale as extensões do sistema de segurança de endpoint que não são mais necessárias e reinicie o conector.
15	A extensão do sistema requer acesso total ao disco	A extensão do sistema requer acesso total ao disco	As extensões de sistema macOS do conector Mac não podem acessar arquivos do usuário para verificação. Abra as preferências do Security & Privacy System e conceda acesso total ao disco à *extensão de segurança AMP*. Detalhes adicionais, incluindo configurações de perfil MDM para autorização remota de acesso total ao disco com extensões de sistema, estão disponíveis nesta nota técnica. Observe que um bug no macOS 11.0.0 pode fazer com que a configuração de acesso total ao disco seja removida espontaneamente em uma reinicialização depois de concedida. Este bug foi corrigido no macOS 11.0.1.
17	Acesso ao Disco Compl	Acesso ao Disco Completo Orbital Não	O orbital requer acesso total ao disco para acessar arquivos e diretórios protegidos para consultas. Abra as preferências do Security & Privacy System e conceda acesso total ao disco ao *Cisco Orbital*.

eto
Orbital
Não Concedido
Conce
dido