Défaillances du connecteur Mac du point de terminaison sécurisé Cisco

Contenu

Introduction

Le connecteur peut vous avertir d'un événement Fault Raised lorsqu'il détecte une condition qui affecte le bon fonctionnement du connecteur. De même, un événement Fault Cleared indique que la condition n'est plus présente.

Table des défaillances du connecteur

Le tableau suivant décrit les pannes et les étapes de diagnostic correspondantes.

ID de panne	Texte du portail	Point de terminaison Description	Dépannage/Résolution
1	Module de noyau non autorisé	Extension du système non autorisée	L'extension système du connecteur n'a pas pu être exécutée. Ouvrez les Préférences du système de sécurité et de confidentialité et approuv l'extension. Vous pouvez également approuver les extensions système à distance à l'aide profil de [gestion des appareils mobiles (MDM)](#).
2	Incompatibilité de version	Incompatibilité de la version de l'extension système	Le logiciel Connector installé est endommagé. Réinstallez le connecteur. Remarque : lors de l'exécution de Mac Connector versions 1.14.0 et ultérieure est possible de résoudre certains problèmes en redémarrant l'ordinateur.
3	Accès au disque non accordé	Accès au disque complet non accordé	Le connecteur ne peut pas accéder aux fichiers utilisateur pour analyse. Ouvre préférences du système de sécurité et de confidentialité et accordez l'accès complet au disque au service AMP. Pour les versions antérieures à 1.14.0 du connecteur Mac, ce processus est nommé */opt/cisco/amp/ampdaemon*. Pour les versions 1.14.0 et ultérieures de Mac Connector, les deux application suivantes nécessitent un accès complet au disque en fonction de la version m : • *AMP pour les points terminaux Service* (nécessaire pour toutes les versio macOS) • *Extension de sécurité AMP* (requis sur macOS 10.15.5 et versions ultérieu Pour les versions 1.14.1 et ultérieures de Mac Connector, les deux application suivantes nécessitent un accès complet au disque en fonction de la version m : • *AMP pour les points terminaux Service* (nécessaire pour toutes les versio

			macOS) • *Extension de sécurité AMP* (requis sur macOS 11 et versions ultérieures) Des détails supplémentaires sont disponibles dans cette note technique.
4	Module de noyau non chargé	Impossible de charger l'extension système ; réinstaller le connecteur	Pour les versions de Mac Connector antérieures à la version 1.14.0, ou lors de l'exécution sur macOS 10.14 ou 10.15, cette erreur indique que l'extension sys de Connector est la version correcte et a été approuvée pour exécution mais n toujours pas pu être chargée. Consultez */Library/Logs/Cisco/ampdaemon.log* p plus de détails. La désinstallation et la réinstallation du connecteur peuvent également effacer cette erreur.
5	Utilisateur du service d'analyse non disponible	Utilisateur du service d'analyse non disponible	Le connecteur n'a pas pu créer un utilisateur pour exécuter le processus d'ana de fichiers. Le connecteur s'en sert pour analyser les fichiers à l'aide de l'utilisa racine. Cela dévie de la conception prévue et n'est pas prévu. Si la `cisco-amp-scan-svc` l'utilisateur ou le groupe a été supprimé, ou la configur de l'utilisateur et du groupe a été modifiée, la réinstallation du connecteur recr l'utilisateur et le groupe avec la configuration nécessaire. Pour plus d'informati reportez-vous à la section */Library/Logs/Cisco/ampdaemon.log*.
6	Redémarrage fréquent du service d'analyse	Redémarrage fréquent du service d'analyse	Le processus d'analyse des fichiers du connecteur a rencontré des échecs rép et le connecteur a redémarré pour tenter de supprimer l'échec. Il est possible q ou plusieurs fichiers du système provoquent un plantage de l'algorithme d'ana lors de l'analyse. Le connecteur poursuit les analyses au mieux. Si ce défaut n'est pas automatiquement résolu dans les 10 minutes qui suivent démarrage du connecteur, cela indique que l'intervention de l'utilisateur est nécessaire et que la capacité du connecteur à effectuer des analyses est dégr Revoir */Library/Logs/Cisco/ampdaemon.log* et */Library/Logs/Cisco/ampscansv* pour plus de détails.
7	Échec du démarrage du service d'analyse	Échec du démarrage du service d'analyse	Le processus d'analyse de fichier du connecteur n'a pas pu démarrer et le connecteur a redémarré pour tenter d'effacer l'échec. La fonctionnalité d'analy fichiers est désactivée lorsque cette erreur est déclenchée. Cet échec peut être déclenché si une erreur se produit lors du chargement d'u fichier de définition de virus nouvellement installé (.cvd files). Le connecteur effectue un certain nombre de vérifications d'intégrité et de stabilité avant d'act de nouveaux fichiers .cvd pour éviter cette défaillance. Au redémarrage, le connecteur supprime tous les fichiers .cvd non valides afin que le connecteur puisse reprendre. Si ce défaut n'est pas résolu lors du redémarrage du connecteur, cela indique l'intervention de l'utilisateur est requise. Si cet échec se répète avec chaque m jour .cvd, cela indique qu'un fichier .cvd non valide n'est pas correctement déte par les vérifications d'intégrité du fichier .cvd du connecteur. Revoir */Library/Logs/Cisco/ampdaemon.log* et */Library/Logs/Cisco/ampscansv* pour plus de détails.
10	Redémarrage requis pour charger le	Redémarrage requis pour charger les extensions système	Redémarrez le système. Pour les versions 1.11.1 et 1.14.0 du connecteur Mac, cette erreur peut être soulevée si les extensions système ne peuvent pas se charger. Dans ce cas, v pouvez remédier à ce problème en réinstallant le connecteur. Notez que Mac Connector 1.14.1 et versions ultérieures peut provoquer cette

	module du noyau ou l'extension du système		si trop d'extensions système de filtre de contenu réseau sont installées sur le système. Reportez-vous au guide de panne 13 ci-dessous pour plus de détails redémarrage de l'ordinateur ne supprime pas ce problème.
12	Filtre réseau non autorisé	Filtre réseau non autorisé	Le filtre réseau est requis par la fonction Activer la corrélation de flux de périphériques de la stratégie. Pour supprimer cette erreur, autorisez le service for Endpoints à filtrer le contenu réseau sur le point d'extrémité. La boîte de dialogue macOS permettant d'autoriser le filtre réseau est accessil cliquant sur la défaillance active répertoriée dans le menu Agent et en suivant instructions fournies. Des détails supplémentaires, notamment les paramètres de profil MDM pour l'autorisation à distance des filtres réseau, sont disponibles dans cette note technique.
13	Trop d'extensions système de filtrage de contenu réseau	Trop d'extensions système de filtrage de contenu réseau	Pour Mac Connector 1.14.0, cette erreur est fréquemment soulevée en raison bogue macOS lors du démarrage de l'extension du système de filtre de conter réseau. Si vous redémarrez l'ordinateur, ce problème sera résolu. La fonctionnalité Activer la corrélation de flux de périphérique de la stratégie nécessite l'utilisation d'un filtre de contenu réseau macOS de type pare-feu. MacOS limite le nombre de filtres de contenu réseau pouvant être exécutés. Si ce problème est déclenché et n'est pas résolu en redémarrant l'ordinateur, désinstallez les filtres de contenu réseau de niveau pare-feu qui ne sont plus nécessaires et redémarrez le connecteur.
14	Trop d'extensions de système de sécurité de point d'extrémité	Trop d'extensions système de sécurité des terminaux	MacOS limite le nombre d'extensions système de sécurité des points de terminaison pouvant être exécutées. Le connecteur Mac nécessite l'une de ce extensions système de sécurité des points d'extrémité pour les fonctions Surveillance des copies et des déplacements de fichiers et Surveillance de l'exécution de processus dans la stratégie. Pour supprimer cette erreur, désinstallez les extensions système de sécurité d points d'extrémité qui ne sont plus nécessaires et redémarrez le connecteur.
15	L'extension système nécessite un accès complet au disque	L'extension système nécessite un accès complet au disque	Les extensions système macOS du connecteur Mac ne peuvent pas accéder a fichiers utilisateur pour analyse. Ouvrez les préférences du système de sécurit de confidentialité et accordez l'accès complet au disque à l'*extension de sécur AMP*. Des détails supplémentaires, notamment les paramètres de profil MDM pour l'autorisation à distance de l'accès complet au disque avec les extensions syst sont disponibles dans cette note technique. Notez qu'un bogue sur macOS 11.0.0 peut provoquer l'effacement spontané d paramètre d'accès au disque complet lors d'un redémarrage après son octroi. bogue a été corrigé dans macOS 11.0.1.
17	Accès	Accès au	Orbital nécessite un accès complet au disque pour accéder aux fichiers et

au disque complet orbital non accordé	disque complet orbital non accordé	répertoires protégés pour les requêtes. Ouvrez les préférences du système de sécurité et de confidentialité et accordez l'accès complet au disque à *Cisco Or*