Cisco Secure Endpoint Macコネクタの障害

内容

概要

コネクタがコネクタの適切な機能に影響を与える状態を検出すると、Fault Raisedイベントが通知されることがあります。同様に、Fault Clearedイベントは、その状態が解消されたことを通知します。

コネクタ障害テーブル

次の表に、障害と対応する診断手順を示します。

障害ID	ポータルテキスト	エンドポイント説明	トラブルシューティング/解決
1	カーネルモジュールが承認されていません	システム拡張が承認されていません	コネクタのシステム拡張の実行がブロックされました。 [Security and Privacy System Preferences]を開き、内線を承認します。 または、モバイルデバイス管理(MDM)プロファイルを使用してシステム拡張をートで承認することもできます。
0	バージョンのミスマッチ	システム拡張バージョンの不一致	インストールされているコネクタソフトウェアが破損しています。コネクタをンストールします。 注：Mac Connectorバージョン1.14.0以降を実行している場合、コンピュータ起動すると、この障害の一部がクリアされる可能性があります。
3	ディスクアクセスが許可されていません	フルディスクアクセスは許可されていません	コネクタはスキャンのためにユーザーファイルにアクセスできません。[Secuand Privacy System Preferences]を開き、AMPサービスへのフルディスクアクを許可します。 1.14.0より前のバージョンのMac Connectorでは、このプロセスは*/opt/cisco/amp/ampdaemonという名前です*。 Mac Connectorバージョン1.14.0以降では、次の2つのアプリケーションはmacOSのバージョンに応じてフルディスクアクセスを必要とします。 • *AMP for Endpoints サービス*（すべてのmacOSバージョンに必要） • *AMPセキュリティ拡張* (macOS 10.15.5以降で必要) Mac Connectorバージョン1.14.1以降では、次の2つのアプリケーションはmacOSのバージョンに応じてフルディスクアクセスを必要とします。 • *AMP for Endpoints サービス*（すべてのmacOSバージョンに必要） • *AMPセキュリティ拡張*（macOS 11以降で必要） 詳細については、このテクニカルノートを参照してください。
4	カーネルモジュール	システム拡張を読み込めませんで	1.14.0より前のバージョンのMacコネクタ、またはmacOS 10.14または10.15行されている場合、このエラーは、Connectorのシステム拡張が正しいバージであり、実行が承認されているが、ロードに失敗したことを示します。詳細に

	がロードされていません	した。コネクタを再インストールします	ては*/Library/Logs/Cisco/ampdaemon.log*を参照してください。コネクタをアンストールして再インストールすると、この障害が解消される場合があります。
5	スキャンサービスユーザが使用できません	スキャンサービスユーザが使用できません	コネクタは、ファイルスキャンプロセスを実行するユーザーを作成できませんた。Connectorは、これを回避するためにrootユーザを使用してファイルスキを実行します。これは意図した設計から逸脱しており、予期されていません。 If the `cisco-amp-scan-svc` ユーザーまたはグループが削除されたか、ユーザーとープの構成が変更されました。コネクタを再インストールすると、必要な構成ーザーとグループが再作成されます。詳細については、*/Library/Logs/Cisco/ampdaemon.log*.
6	サービスの再起動が頻繁に発生する	サービスの再起動が頻繁に発生する	コネクタのファイルスキャンプロセスで繰り返しエラーが発生し、コネクタはーをクリアするために再起動しました。システム上の1つ以上のファイルがスン時にスキャンアルゴリズムのクラッシュを引き起こしている可能性がありまコネクタはベストエフォート方式でスキャンを続行します。 コネクタの起動後10分以内にこの障害が自動的にクリアされない場合は、さらユーザの介入が必要であり、コネクタのスキャン実行能力が低下することを示す。 詳細については、『 */Library/Logs/Cisco/ampdaemon.log* と */Library/Logs/Cisco/ampscansvc.log* を参照してください。
7	スキャンサービスを開始できませんでした	スキャンサービスを開始できませんでした	コネクタのファイルスキャンプロセスを開始できませんでした。エラーをクリるためにコネクタが再起動されました。この障害が発生している間、ファイルャン機能は無効になります。 このエラーは、新しくインストールされたウイルス定義ファイル（.cvdファイ）の読み込み中にエラーが発生した場合に発生する可能性があります。 コネクは、この障害を防ぐために、新しい.cvdファイルをアクティブ化する前に、整と安定性のチェックをいくつも実行します。再起動時に、コネクタは無効な.cァイルをすべて削除し、コネクタを再開できるようにします。 コネクタの再起動時にこの障害が解消されない場合は、ユーザによる追加の介必要であることを示します。この障害が.cvdアップデートごとに繰り返される、無効な.cvdファイルがConnectorの.cvdファイル整合性チェックによって正検出されていないことを示しています。 詳細については、『 */Library/Logs/Cisco/ampdaemon.log* と */Library/Logs/Cisco/ampscansvc.log* を参照してください。
10	カーネルモジュールまたはシステム拡張を読み込むために必要な再起動	システム拡張をロードするために再起動が必要	システムをリブートします。 Mac Connectorバージョン1.11.1および1.14.0では、システム拡張がロードでい場合にこの障害が発生する可能性があります。この場合、コネクタを再インールすると、この障害を解消できます。 Mac Connector 1.14.1以降では、システムにインストールされているNetwork Content Filter（Nコンテンツフィルタ）システム拡張が多すぎると、この障害生する可能性があることに注意してください。コンピュータをリブートしてもの障害が解消されない場合は、次の障害13のガイダンスを参照してください。
12	ネットワーク	ネットワークフィルタ	ネットワークフィルタは、ポリシーの[デバイスフロー相関の有効化]機能で必す。この障害をクリアするには、「AMP for Endpoints Service」がエンドポイ

			のネットワークコンテンツをフィルタリングできるようにします。
	フィルタは許可されていません	は許可されていません	ネットワークフィルタを許可するmacOSダイアログにアクセスするには、Ag menuletにリストされているアクティブな障害をクリックし、表示されている ダンスに従います。 ネットワークフィルタのリモート承認用のMDMプロファイル設定などの詳細 いては、次のリンクを参照してください。 このテクニカルノート。
13	ネットワークコンテンツフィルタシステムの拡張機能が多すぎます	ネットワークコンテンツフィルタシステムの拡張機能が多すぎます	Mac Connector 1.14.0では、ネットワークコンテンツフィルタシステム拡張の 時にmacOSのバグが原因で、この障害が頻繁に発生します。コンピュータを 動すると、この障害は解消されます。 ポリシーの[デバイスフロー相関の有効化(Enable Device Flow Correlation)]機 は、ファイアウォールグレードのmacOSネットワークコンテンツフィルタを する必要があります。MacOS 実行できるネットワークコンテンツフィルタの 制限します。 この障害が発生し、コンピュータをリブートしてもクリアされない場合必要な ったファイアウォールグレードのネットワークコンテンツフィルタをアンイン ールし、コネクタを再起動します。
14	エンドポイントセキュリティシステムの拡張が多すぎます	エンドポイントセキュリティシステムの拡張が多すぎます	MacOSは、実行できるエンドポイントセキュリティシステム拡張の数を制限 す。Macコネクタには、ポリシーの「Monitor File Copies and Moves」および Monitor Process Execution」機能に対して、次のいずれかのエンドポイントセ リティシステム拡張が必要です。 このエラーをクリアするには、不要になったEndpoint Securityシステム拡張を インストールし、コネクタを再起動します。
15	システム拡張にはフルディスクアクセスが必要	システム拡張にはフルディスクアクセスが必要	Mac ConnectorのmacOSシステム拡張は、スキャンのためにユーザファイルに セスできません。[Security & Privacy System Preferences]を開き、AMPセキュ ィ拡張へのフルディスクアクセスを*許可します*。 システム拡張を使用したフルディスクアクセスのリモート承認のためのMDM ファイル設定などの詳細については、このテクニカルノートを参照してくださ macOS 11.0.0のバグが原因で、許可された後のリブート時にフルディスクア ス設定が自動的にクリアされる可能性があることに注意してください。この macOS 11.0.1で修正されています。
17	軌道フルディスクアクセスが許可されていません	軌道フルディスクアクセスが許可されていません	オービタルでは、保護されたファイルやディレクトリにアクセスしてクエリを するためにフルディスクアクセスが必要です。[Security & Privacy System Preferences]を開き、Cisco Orbitalにフルディスクアクセスを*許可します*。