Secure Endpoint Linuxコネクタの障害のトラブルシューティング

内容

はじめに

このドキュメントでは、Cisco Secure Endpoint Linuxコネクタが正常な機能に影響を与える状態を通知するために使用する障害について説明します。

背景説明

Cisco Secure Endpoint Linuxコネクタは、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イベントを通知します。同様に、Fault Clearedイベントは、この状態が解消されたことを通知します。

セキュアエンドポイントLinuxコネクタの障害テーブル

次の表に、障害と関連する診断手順を示します。

障害ID	説明	トラブルシューティング/解決
5	スキャンサービスのユーザーが利用できません	コネクタは、ファイルスキャンプロセスを実行するためのユーザーを作成できませんでした。コネクタは回避策として、rootユーザを使用してファイルスキャンを実行します。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スキャンSVC` ユーザまたはグループが削除されたか、ユーザおよびグループの設定が変更された場合は、コネクタを再インストールして、必要な設定でユーザおよびグループを再作成できます。その他の詳細については、を参照してください。 /var/log/cisco/ampdaemon.logを参照。 /etc/login.defsの設定でユーザグループの作成が制限されている場合、ユーザとグループの作成を許可するには、インストーラの実行中にこのファイルを一時的に変更する必要があります。これを行うには、

		usergroups_enabをnoからyesに変更します。 このエラーは、Linuxコネクタ1.15.1以降で、他のプログラムがコネクタのディレクトリ権限（/opt/ciscoまたは子ディレクトリ）のいずれかを変更した場合に発生する可能性があります。これを軽減するには、変更したディレクトリ権限をデフォルト（0755など）に戻し、今後のプログラムで/opt/ciscoディレクトリ（または子ディレクトリ）が変更されないことを確認し、コネクタサービスを再起動する必要があります。
6	サービスの再起動を頻繁にスキャンする	コネクタファイルのスキャンプロセスで繰り返しエラーが発生し、エラーをクリアするためにコネクタが再起動されました。システム上の1つ以上のファイルが原因で、スキャン時にスキャンアルゴリズムがクラッシュする可能性があります。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、さらなるユーザ介入が必要であり、コネクタのスキャン実行の機能が低下していることを示しています。 詳細については、/var/log/cisco/ampdaemon.logおよび/var/log/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	コネクタのファイルスキャンプロセスを開始できず、エラーをクリアするためにコネクタが再起動されました。このエラーが発生している間、ファイルスキャン機能は無効になります。 この障害は、新しくインストールされたウイルス定義ファイル（.cvdファイル）のロード時にエラーが発生した場合にトリガーされる可能性があります。コネクタは、新しい.cvdファイルをアクティブ化する前に、整合性と安定性に関するさまざまなチェックを実行して、この障害を回避します。再起動時に、コネクタは無効な.cvdファイルを削除し、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クリアされない場合は、さらなるユーザ介入が必要であることを示しています。この障害が.cvdの更新ごとに繰り返される場合は、無効な.cvdファイルがコネクタの.cvdファイル整合性チェックによって適切に検出されていないことを示しています。 この障害は、マシンの使用可能メモリが不足していて、スキャナサービスを開始できない場合に、Linuxコネクタでトリガーされる可能性があります。Linuxの最小システム要件については、『Secure Endpoint (formerly AMP for Endpoints) User Guide』を参照してください。 詳細については、/var/log/cisco/ampdaemon.logおよび/var/log/cisco/ampscansvc.logを参照してください。

8	リアルタイムファイルシステムモニタを開始できませんでした	リアルタイムのファイルシステムアクティビティの監視を提供するカーネルモジュールが読み込まれず、コネクタポリシーで[ファイルのコピーと移動を監視する]が有効になっています。この障害が発生している間、これらのモニタリング機能はコネクタで使用できません。このエラーは、Secure Endpoint Connectorがファイルシステムアクティビティの監視に必要な基盤となるカーネルモジュールをロードできない場合に発生します。 UEFIセキュアブートをシステムで無効にする必要があります。 セキュアブートが無効になっている場合は、セキュアエンドポイントコネクタに付属のampavfltまたはampfsmカーネルモジュールと、システムにインストールされているシステムカーネルまたはその他のサードパーティカーネルモジュールとの間に互換性がないことが原因である可能性があります。詳細については、/var/log/messagesを参照してください。 この障害は、コネクタでサポートされていないカーネルバージョンを実行している場合にも発生する可能性があります。この場合、現在実行中のシステムカーネル用のカスタムampfsmカーネルモジュールを構築することでクリアできます。（Linuxコネクタバージョン1.16.0以降に適用されます）。 カスタムカーネルモジュールの構築の詳細については、「Cisco Secure Endpoint Linuxコネクタカーネルモジュールの構築」を参照してください。
9	リアルタイムネットワークモニターを開始できませんでした	ネットワークアクティビティのリアルタイムモニタリングを提供するカーネルモジュールが読み込まれず、コネクタポリシーで[デバイスフローの関連付けを有効にする]が有効になっています。この障害が発生している間、この監視機能はコネクタでは使用できません。 このエラーは、Secure Endpoint Connectorがファイルシステムアクティビティの監視に必要な基盤となるカーネルモジュールをロードできない場合に発生します。 UEFIセキュアブートをシステムで無効にする必要があります。 セキュアブートが無効になっている場合は、セキュアエンドポイントコネクタに付属のampavfltまたはampfsmカーネルモジュールと、システムにインストールされているシステムカーネルまたはその他のサードパーティカーネルモジュールとの間に互換性がないことが原因である可能性があります。詳細については、/var/log/messagesを参照してください。 この障害は、コネクタでサポートされていないカーネルバージョンを実行している場合にも発生する可能性があります。この場合、現在実行中のシステムカーネル用のカスタムampfsmカーネルモジュールを構築することでクリアできます。（Linuxコネクタバージョン1.16.0以降に適用されます）。 カスタムカーネルモジュールの構築の詳細については、「Cisco Secure Endpoint Linuxコネクタカーネルモジュールの構築」を参照してください。

11	必要なカーネルデバイスパッケージがありません	セキュアエンドポイントコネクタは、eBPFモジュールを使用して、ファイルシステム、プロセス、およびネットワークアクティビティを監視します。コネクタでは、これらのeBPFモジュールをロードして実行するために、特定のパッケージがシステムで使用可能になっている必要があります。このエラーを解決するには、次の手順に従ってLinuxディストリビューションに必要なパッケージをインストールし、コネクタを再起動します。 Red Hatベースのディストリビューションでは、カーネル開発パッケージが欠落している場合、このエラーが発生します。kernel-develパッケージをインストールし、コネクタを再起動します。（Linuxコネクタバージョン1.13.0以降にのみ適用可能）。 Oracle Linux UEK 6以降では、このエラーはkernel-uek-develパッケージが見つかりません。kernel-uek-develパッケージをインストールし、コネクタを再起動します。（Linuxコネクタバージョン1.18.0以降にのみ適用可能）。 Debianベースのディストリビューションでは、linux-headersパッケージが見つからないときにこのエラーが発生します。linux-headersパッケージをインストールし、コネクタを再起動します。（Linuxコネクタバージョン1.15.0以降に適用されます）。 詳細については、次のサイトを参照してください。 Linuxカーネルデバイスの障害
16	互換性のないカーネル	現在実行中のカーネルは現在実行中のコネクタと互換性がなく、コネクタポリシーで[ファイルのコピーと移動を監視する]または[デバイスフローの関連付けを有効にする]が有効になっています。 カーネルをサポートされているバージョンにダウングレードするか、このカーネルをサポートする新しいバージョンにコネクタをアップグレードします。 サポートされているカーネルのバージョンの詳細については、以下を参照してください。 Cisco Secure Endpoint LinuxコネクタのOS互換性
18	コネクタイベント監視が過負荷です	このエラーは、多数のシステムイベントが原因でコネクタに大きな負荷がかかっているときに発生します。システムの保護は制限されており、システム全体のアクティビティが減少するまで、コネクタは比較的小さなシステムクリティカルイベントのセットを監視します。 このエラーは、悪意のあるシステムアクティビティまたはシステム上の非常にアクティブなアプリケーションを示している可能性があります。 アクティブなアプリケーションが良性で、ユーザーによって信頼されている場合、そのアプリケーションをプロセス除外セットに追加して、コネクタの監視負荷を軽減できます。このアクションは、エラーを解消するのに

		十分な場合があります。 悪意のないプロセスが大きな負荷を引き起こさない場合は、アクティビティの増加が悪意のあるプロセスによるものかどうかを判断するために何らかの調査が必要です。 コネクタに短期間の高負荷が発生した場合は、この障害が自然に解消される可能性があります。 このエラーが頻繁に発生し、負荷が大きい問題のないプロセスがなく、悪意のあるプロセスが見つからない場合は、負荷が大きいシステムを再プロビジョニングする必要があります。
19	SELinuxポリシーが見つからないか、無効になっています	このエラーは、システムのSecure Enterprise Linux(SELinux)ポリシーによってコネクタがシステムアクティビティを監視できなくなったときに発生します。SELinuxが有効でenforcingモードの場合、コネクタはSELinuxポリシーで次のルールを要求します。 `allow unconfinded_service_t self:bpf { map_create map_read map_write prog_load prog_run };` RHEL 7およびOracle Linux 7を含むRed Hatベースのシステムでは、このルールはデフォルトのSELinuxポリシーには存在しません。インストールまたはアップグレード時に、コネクタは次の名前のSELinuxポリシーモジュールのインストールを介してこの規則を追加しようとします `Ciscoセキュア`BPFを参照。もし `Ciscoセキュア`BPF インストールとロードに失敗するか、無効になると、エラーが発生します。 このエラーを解決するには、システムパッケージpolicycoreutils-pythonがインストールされていることを確認します。コネクタを再インストールまたはアップグレードして`cisco-secure-bpf`のインストールをトリガーするか、既存のSELinuxポリシーにルールを手動で追加し、コネクタを再起動します。 SELinuxポリシーを変更してこの障害を解決する方法の詳細については、「SELinuxポリシーの障害」を参照してください。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。