セキュアエンドポイントによって隔離されたファイルの回復

内容

はじめに

このドキュメントでは、セキュアエンドポイントコネクタによって隔離されたファイルをセキュアエンドポイントコンソールから復元する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Secure Endpointコンソール

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

- セキュアエンドポイントコンソールv5.4.2025030619

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

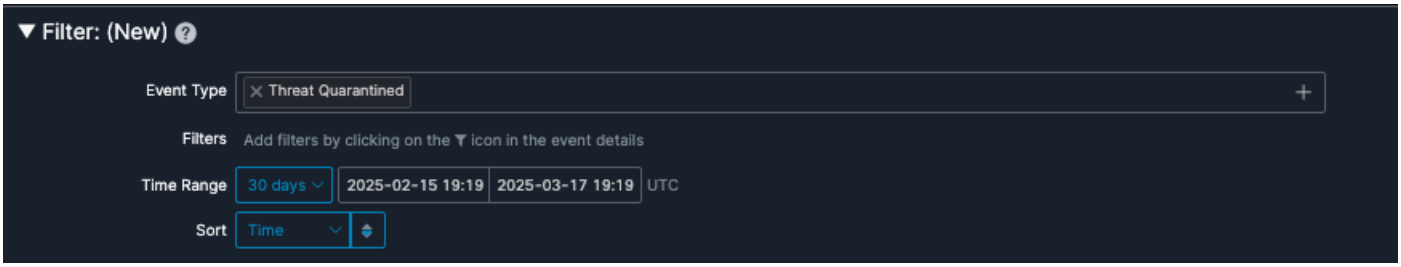
問題

Secure Endpoint(SE)コネクタによって検疫されたファイルは、ファイル分析、誤検出の送信、またはファイルが安全であると判明した場合の復元のために取得できます。管理者は、Secure Endpoint Consoleからこの操作を直接実行できます。

解決方法

1. SEコンソールのEventsページに移動します。

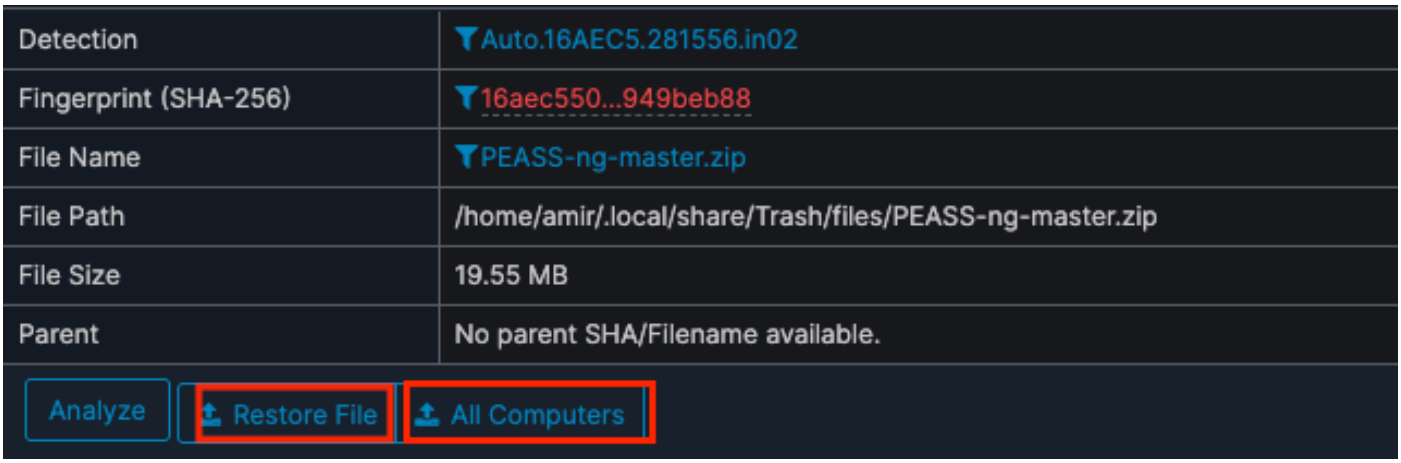
2. フィルタ「Event Type = Threat Quarantined」を選択して、イベントをフィルタリングし、成功した隔離をすべて表示します。



脅威の隔離されたイベントタイプ

3. 復元するファイルに関連付けられている検出イベントを識別します。

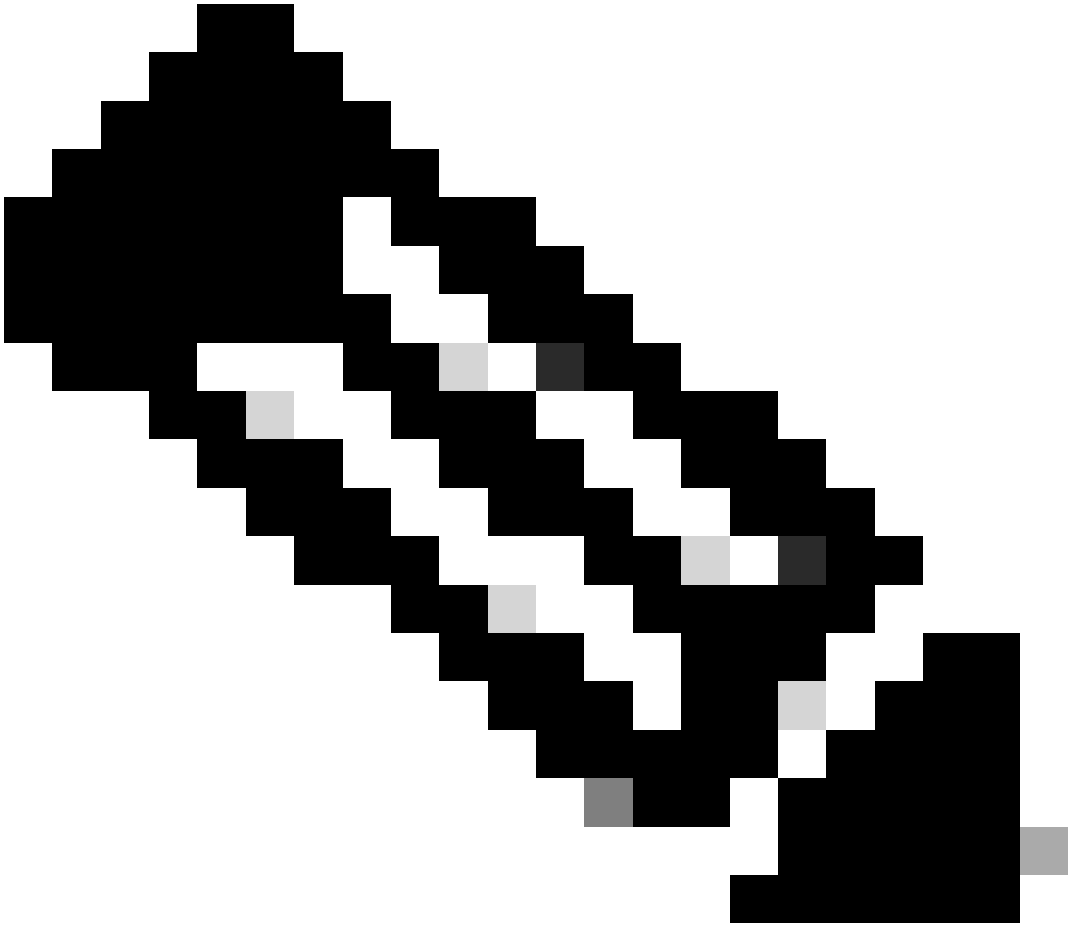
4. イベントの詳細を展開し、「ファイルの復元」オプションにアクセスします。 Restore Fileを選択すると、影響を受けるマシンのファイルが復元されます。All Computersを選択すると、隔離されたすべてのマシンのファイルが復元されます。



ファイルの復元オプション

5. ハートビート間隔とは、管理者が復元するファイルがあるかどうかを確認するためにコネクタがホームを呼び出す頻度です。 影響を受けたコンピュータがオンラインになるか、次のハートビート間隔が発生すると、ファイルが復元されます。

6. ファイルが信頼できる場合は、そのファイルを許可リストに追加して、再び隔離されないようにします。



注：ファイルは30日間隔離されたままになるか、隔離フォルダが100 MBに達して最も古いファイルが削除されます。隔離されたファイルは、パージ後にリストアできなくなります。

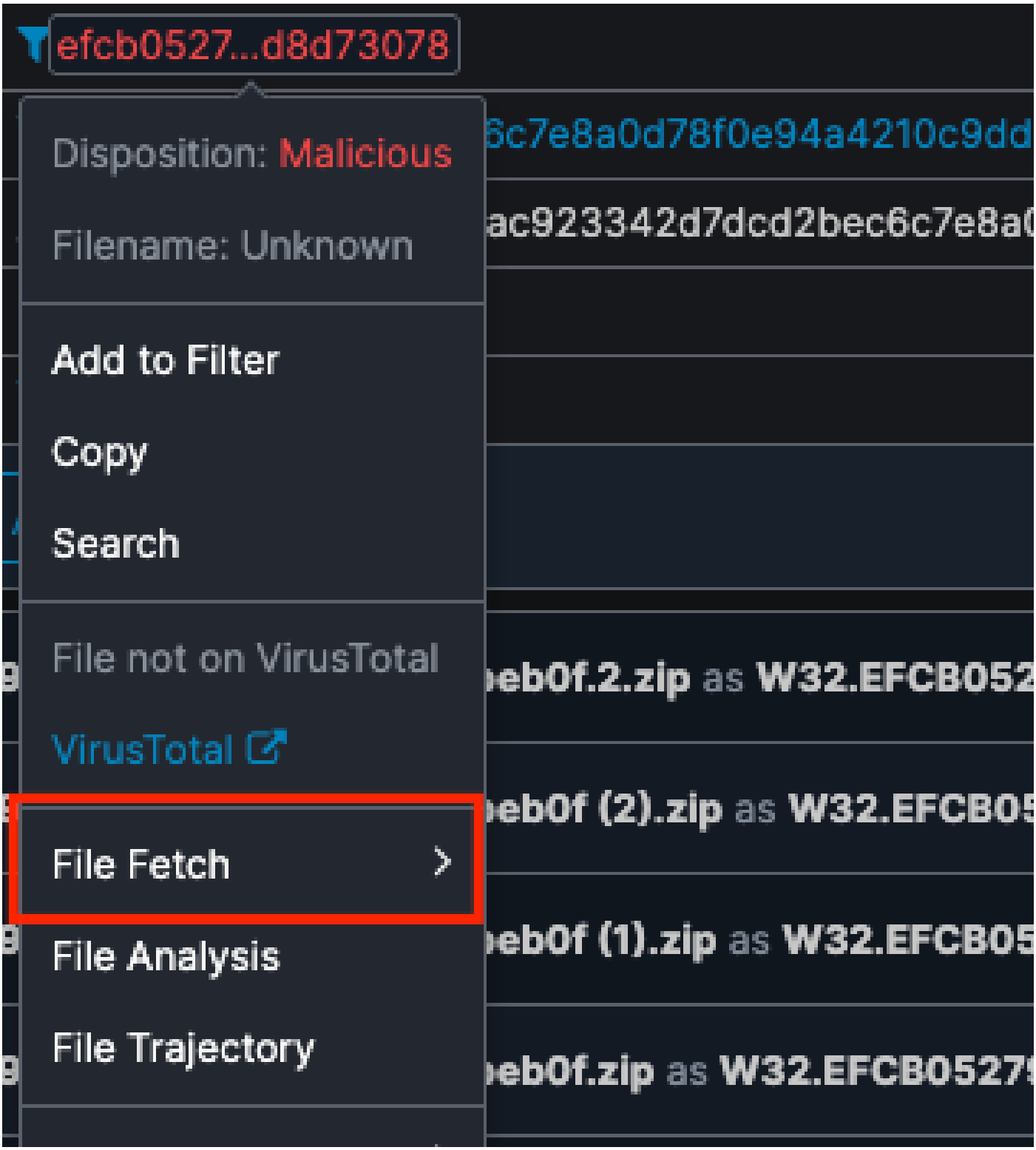
脅威分析または誤検出の送信のために隔離されたファイルを環境に復元せずにダウンロードする必要がある場合は、ファイルフェッチ機能を使用できます。 隔離されたファイルのダウンロード手順：

1. SEコンソールのEventsページに移動します。

2. フィルタ「Event Type = Threat Quarantined」を選択して、イベントをフィルタリングし、成功した隔離をすべて表示します。

3. ダウンロードするファイルに関連する検出イベントを特定します。

4. 隔離されたファイルのSHA-256値をクリックして、File Fetchオプションを表示します。



ファイルフェッチ

これにより、ファイルフェッチのステータス、フェッチを開始するオプション、ファイルリポジトリ内のファイルを表示するためのアクセスが提供されます。

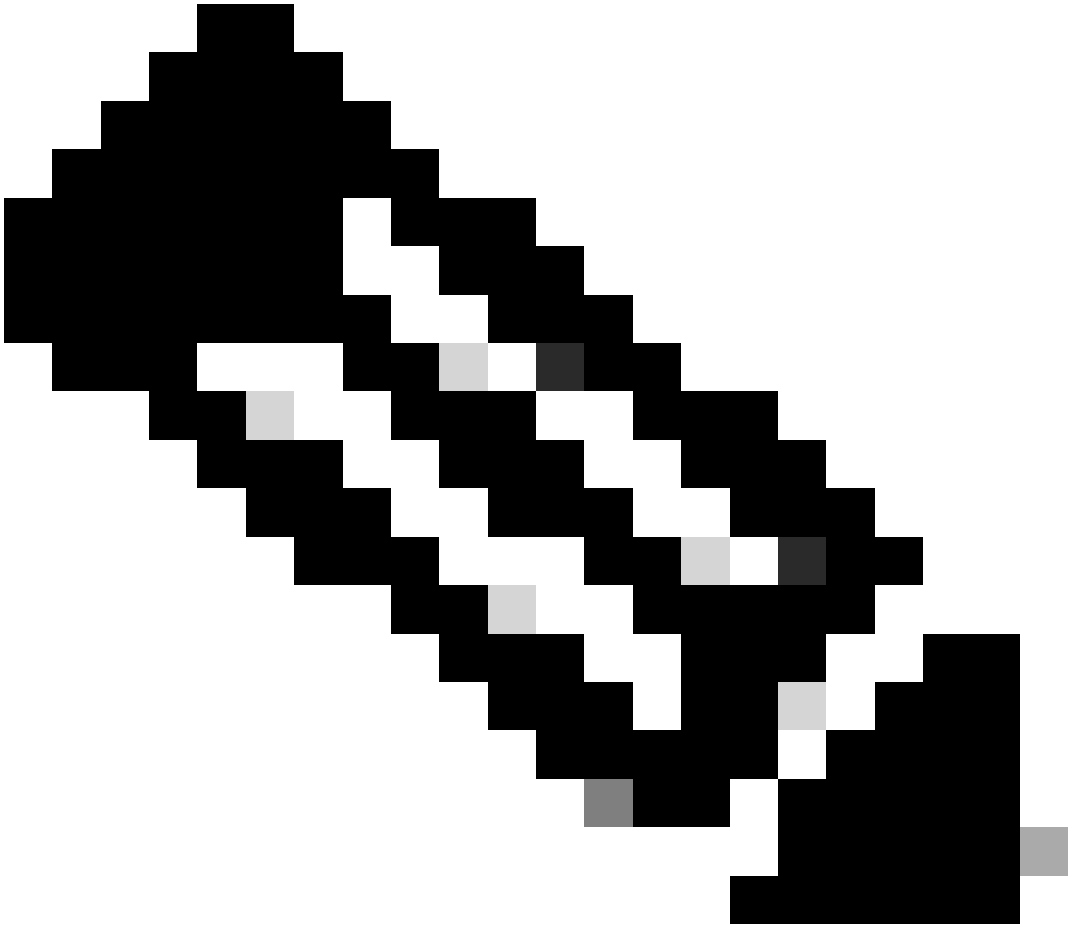
5. Fetch Fileをクリックし、ファイルを取得するComputerを選択し、Fetchをクリックして確認します。

6. ファイルがファイルリポジトリにアップロードされると、電子メール通知が送信されます。

7. ファイルが使用可能になると、Analysis> File Repositoryでそのファイルとダウンロードするオプションを確認できます。

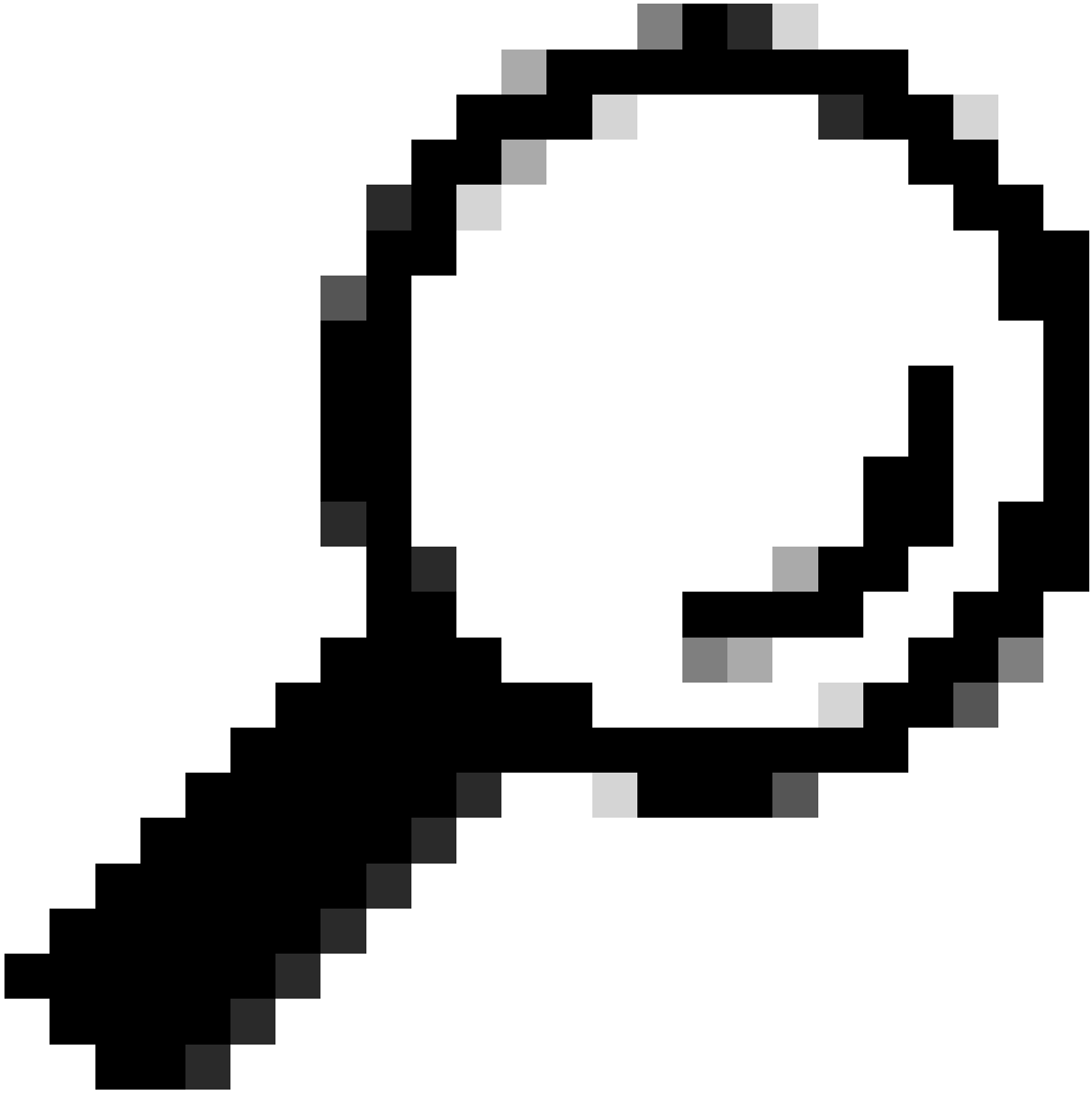
ファイルのダウンロード

ファイルリポジトリからダウンロードされたすべてのファイルはzip形式で圧縮され、パスワードで保護されます。



注：ファイルフェッチが正しく機能するには、ネットワークトラフィックが、クラウドの地域(ヨーロッパ：rff.eu.amp.cisco.com、北米：rff.amp.cisco.com、APJC:rff.apjc.amp.cisco.com)に基づいて、適切なファイルフェッチサーバに許可されている必要があります。また、ファイルフェッチ要求を正常に開始するために必要なAdministratorアカウントに対して、2要素認証(2FA)が有効になっていることを確認します

。



ヒント:Event Type = Quarantined Restore FailedおよびEvent Type = File Fetch Failedを使用してイベントをフィルタリングすることで、障害を特定し、対応する復元操作およびファイルフェッチ操作の理由をそれぞれ確認できます。

上記の手順でファイルを復元できない場合は、Cisco TACに連絡して、C:\Program Files\Cisco\AMP\Quarantineディレクトリにある.qrtファイルを提供してください。

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。