



トラブルシューティング

以下のトピックは、発生する可能性のある問題を診断する方法について説明します。

- [トラブルシューティングのベストプラクティス \(1 ページ\)](#)
- [システム メッセージ \(2 ページ\)](#)
- [基本的なシステム情報の表示 \(5 ページ\)](#)
- [システムメッセージの管理 \(6 ページ\)](#)
- [ヘルスマニターアラートのメモリ使用率しきい値 \(10 ページ\)](#)
- [ディスク使用率とイベントドレインの正常性モニターアラート \(12 ページ\)](#)
- [トラブルシューティング用のヘルスマニターレポート \(16 ページ\)](#)
- [一般的なトラブルシューティング \(19 ページ\)](#)
- [接続ベースのトラブルシューティング \(19 ページ\)](#)
- [Secure Firewall Threat Defense デバイスの高度なトラブルシューティング \(20 ページ\)](#)
- [機能固有のトラブルシューティング \(30 ページ\)](#)

トラブルシューティングのベストプラクティス

- 問題の修正を試みるために変更を加える前に、トラブルシューティングファイルを生成して元の問題をキャプチャします。[トラブルシューティング用のヘルスマニターレポート \(16 ページ\)](#) およびサブセクションを参照してください。

サポートのために Cisco TAC に連絡する必要がある場合に、このトラブルシューティングファイルが必要になることがあります。

- メッセージセンターのエラーメッセージと警告メッセージを調べて、調査を開始します。[システム メッセージ \(2 ページ\)](#) を参照してください
- お使いの製品の製品ドキュメントページの「Troubleshoot and Alerts」という見出しの下にある、該当するテクニカルノートとその他のトラブルシューティングリソースを探します。

システムメッセージ

システムで発生した問題を突き止める必要がある場合、調査の出発点となるのはメッセージセンターです。メッセージセンターでは、システムがシステムのアクティビティとステータスに関して継続的に生成するメッセージを表示できます。

メッセージセンターを開くには、メインメニューの [展開 (Deploy)] メニューの隣にある [システムステータス (System Status)] アイコンをクリックします。このアイコンは、システムのステータスによって以下のように表示されます。

-  : 1つ以上のエラーと任意の数の警告がシステム上に存在することを示します。
-  : 1つ以上の警告がシステム上に存在することを示します。エラーは発生していません。
-  : 警告とエラーはいずれもシステム上に存在していないことを示します。

アイコンに数字が表示されている場合、その数字は現在のエラーメッセージまたは警告メッセージの数を示します。

メッセージセンターを閉じるには、Web インターフェイス内でメッセージセンターの外側をクリックします。

メッセージセンターに加え、Web インターフェイスには、ユーザーのアクティビティおよび進行中のシステム アクティビティに応じて即時にポップアップ通知が表示されます。ポップアップ通知のなかには5秒経過すると自動的に非表示になるものや、[表示を消す (Dismiss)]

() をクリックして明示的に表示を消さなければならない「スティッキー」通知もあります。通知リストの最上部にある [表示を消す (Dismiss)] リンクをクリックすると、すべての通知をまとめて非表示にすることができます。



ヒント スティッキー以外のポップアップ通知の上にマウスのカーソルを合わせると、その通知はスティッキーになります。

システムはユーザーのライセンス、ドメイン、アクセスロールに基づいて、どのメッセージをポップアップ通知やメッセージセンターに表示するか決定します。

メッセージタイプ

Message Center では、システムのアクティビティとステータスをレポートするメッセージが3つのタブに編成されて表示されます。

展開 (Deployments)

このタブには、システムの各アプライアンスの設定展開に関連する現在のステータスがドメイン別にグループ化されて表示されます。システムでは、次の展開ステータス値がこのタブでレポートされます。[履歴の表示 (Show History)] をクリックして、展開ジョブに関する追加情報を取得できます。

- [実行中 (Running)] (回転中) : 設定は展開の処理中です。
- [成功 (Success)] : 設定は正常に展開されました。
- [警告 (Warning)] (⚠) : 警告展開ステータスは、警告システムステータスアイコンとともに表示されるメッセージ数に含まれます。
- [失敗 (Failure)] : 設定は展開に失敗しました。展開が必要な設定変更を参照してください。失敗した展開は、エラー システム ステータス アイコンとともに表示されるメッセージ数に含まれます。

アップグレード

このタブには、管理対象デバイスのソフトウェア アップグレード タスクに関連する現在のステータスが表示されます。システムでは、次のアップグレードステータス値がこのタブでレポートされます。

- [進行中 (In progress)] : アップグレードタスクが進行中であることを示します。
- [完了 (Completed)] : ソフトウェア アップグレード タスクが正常に完了したことを示します。
- [失敗 (Failed)] : ソフトウェア アップグレード タスクが完了しなかったことを示します。

ヘルス

このタブには、システムの各アプライアンスの現在のヘルス ステータス情報がドメイン別にグループ化されて表示されます。ヘルス ステータスは、ヘルス モニタリング についてに記載されているように、ヘルス モジュールによって生成されます。システムでは、次の正常性ステータス値がこのタブでレポートされます。

- [警告 (Warning)] (⚠) : アプライアンス上のヘルスモジュールが警告制限を超え、問題が解決されていないことを示します。[ヘルスモニタリング (Health Monitoring)] ページには、これらの状態が[黄色い三角形 (Yellow Triangle)] (⚠) で示されます。警告ステータスは、警告システムステータスアイコンとともに表示されるメッセージ数に含まれます。
- [クリティカル (Critical)] (❗) : アプライアンス上のヘルスモジュールが重大制限を超え、問題が解決されていないことを示します。[ヘルス モニタリング (Health Monitoring)] ページには、これらの状態が[クリティカル (Critical)] (❗) アイコンで示されます。重大ステータスは、エラー システム ステータス アイコンとともに表示されるメッセージ数に含まれます。
- [エラー (Error)] (✖) : アプライアンス上のヘルス モニタリング モジュールに障害が発生し、それ以降、正常に再実行されていないことを示します。[ヘルスモニタリング (Health Monitoring)] ページには、これらの状態がエラーアイコンで示されます。エラーステータスは、エラー システム ステータス アイコンとともに表示されるメッセージ数に含まれます。

[ヘルス (Health)] タブのリンクをクリックして、[ヘルス モニタリング (Health Monitoring)] ページで関連の詳細情報を表示できます。現在のヘルス ステータス状態がない場合、[ヘルス (Health)] タブにメッセージは表示されません。

タスク

特定のタスク (設定のバックアップや更新のインストールなど) は、完了するまで時間がかかる可能性があります。このタブには、これらの長時間実行タスクのステータスが表示され、自分が開始したタスクや、適切なアクセス権がある場合は、システムの他のユーザが開始したタスクが含まれることがあります。このタブには、各メッセージの最新の更新時間に基づいて時系列の逆順にメッセージが表示されます。一部のタスクステータスメッセージには、問題となっているタスクについての詳細情報へのリンクが含まれています。システムでは、次のタスクステータス値がこのタブでレポートされます。

- [待機中 (Waiting)] : 別の進行中のタスクが完了するまで実行を待機しているタスクを示します。このメッセージタイプでは、更新の経過表示バーが表示されます。
- [実行中 (Running)] : 進行中のタスクを示します。このメッセージタイプでは、更新の経過表示バーが表示されます。
- [再試行中 (Retrying)] : 自動的に再試行しているタスクを示します。なお、すべてのタスクの再試行が許可されるわけではありません。このメッセージタイプでは、更新の経過表示バーが表示されます。
- [成功 (Success)] : 正常に完了したタスクを示します。
- [失敗 (Failure)] : 正常に完了しなかったタスクを示します。失敗したタスクは、**エラー システム ステータス アイコン**とともに表示されるメッセージ数に含まれます。
- [停止 (Stopped)] または [中断 (Suspended)] : システムアップデートのために中断されたタスクを示します。停止したタスクを再開することはできません。通常の動作が復元されたら、もう一度タスクを開始してください。
- [スキップ (Skipped)] : 進行中のプロセスによって、タスクの開始が妨げられました。タスクの開始をもう一度試行してください。

新しいタスクが開始されると、新しいメッセージがこのタブに表示されます。タスクが完了すると (成功、失敗、または停止のステータス) 、タスクを削除するまで、このタブには最終ステータスを示すメッセージが引き続き表示されます。[タスク (Tasks)] タブおよびメッセージデータベースがいっぱいにならないように、メッセージを削除することをお勧めします。

メッセージ管理

メッセージセンターから、以下を実行できます。

- ポップアップ通知の表示を選択します。
- システムデータベースからのタスクステータスメッセージをより多く表示します (削除されていないもので利用可能なものがある場合) 。

- すべてのタスクマネージャ通知のレポートをダウンロードします。
- 個々のタスクのステータスメッセージを削除します。（これは、削除されたメッセージを確認できるすべてのユーザに影響します）。
- タスクのステータスメッセージを一括で削除します。（これは、削除されたメッセージを確認できるすべてのユーザに影響します）。



ヒント シスコは、表示に加えてデータベースの不要なデータを削除するために、累積されたタスクのステータスメッセージを [タスク (Task)] タブから定期的に削除することを推奨します。データベースのメッセージ数が 100,000 に到達すると、削除したタスクのステータスメッセージが自動的に削除されます。

基本的なシステム情報の表示

[バージョン情報 (About)] ページには、システムのさまざまなコンポーネントのモデル、シリアル番号、バージョン情報など、アプライアンスに関する情報が示されます。また、シスコの著作権情報も示されます。

手順

ステップ 1 ページ上部のツールバーで、[ヘルプ (Help)] (?) をクリックします。

ステップ 2 [バージョン情報 (About)] を選択します。

アプライアンス情報の表示

手順

システム (⚙) > [構成 (Configuration)] を選択します。

システムメッセージの管理

手順

ステップ1 [Notification (通告)] をクリックして、メッセージセンターを表示します。

ステップ2 次の選択肢があります。

- [展開 (Deployments)] をクリックして、設定の展開に関連するメッセージを表示します。[展開メッセージの表示 \(7 ページ\)](#) を参照してください。展開メッセージを表示するには、管理者ユーザであるか、[デバイス設定の展開権限](#)が必要です。
- [アップグレード (Upgrades)] をクリックして、デバイスアップグレードタスクに関連するメッセージを表示します。「アップグレードメッセージの表示」を参照してください。「[アップグレードメッセージの表示](#)」を参照してください。これらのメッセージを表示するには、管理者ユーザーであるか、[更新 (Updates)] 権限が必要です。

新しい推奨アップグレードバージョンが表示されます。[通知する (Remind Me)] オプションまたは[詳細 (Details)] オプションを使用して、リマインダの設定または詳細情報の表示をそれぞれ選択できます。

- [正常性 (Health)] をクリックして、[Management Center](#) とそれに登録したデバイスの状況に関連するメッセージを表示します。[正常性メッセージの表示 \(8 ページ\)](#) を参照してください。展開メッセージを表示するには、管理者ユーザーであるか、[正常性 (Health)] 権限が必要です。

[正常性モニター (Health monitor)] リンクをクリックすると、[正常性モニター (Health Monitor)] ページに移動できます。

- [タスク (Tasks)] をクリックして、長時間実行タスクに関連するメッセージを表示または管理します。[タスクメッセージの表示 \(9 ページ\)](#) または[タスクメッセージの管理 \(10 ページ\)](#) を参照してください。誰もが自分のタスクを表示できます。他のユーザのタスクを表示するには、管理者ユーザであるか、[他のユーザのタスク表示権限](#)が必要です。[完了したタスクの削除 (Remove completed tasks)] リンクをクリックすると、完了したタスクを通知から削除できます。
- [レポートのダウンロード (Download Report)] アイコンをクリックして、タスクマネージャにおけるすべての通知のレポートを生成します。[CSVのダウンロード (Download CSV)] または [PDFのダウンロード (Download PDF)] を選択してレポートをダウンロードします。
- [通知を表示 (Show Notifications)] スライダをクリックして、ポップアップ通知の表示を有効または無効にします。

展開メッセージの表示

展開メッセージを表示するには、管理者ユーザであるか、**デバイス設定の展開権限**が必要です。

手順

ステップ 1 [Notification (通知)] をクリックして、メッセージセンターを表示します。

ステップ 2 [導入 (Deployments)] をクリックします。

ステップ 3 次の選択肢があります。

- 現在のすべての展開ステータスを表示するには、[total] をクリックします。
- 任意の展開ステータスに関するメッセージのみを表示するには、そのステータスの値をクリックします。
- 展開の経過時間、開始時刻および停止時刻を表示するには、メッセージの時間経過インジケータ (たとえば、[1m 5s]) の上にカーソルを置きます。

ステップ 4 展開ジョブの詳細情報を表示するには、[show deployment history] をクリックします。

[展開の履歴 (Deployment History)] テーブルには、左側の列に展開ジョブが新しい順にリストされています。

a) 展開ジョブを選択します。

右側の列のテーブルには、ジョブに含まれていた各デバイスと、デバイスごとの展開ステータスが表示されます。

b) デバイスからの応答、および展開中にデバイスに送信されたコマンドを表示するには、デバイスの [Transcript] カラムにあるダウンロードアイコンをクリックします。

トランスクリプトには、次のセクションが含まれています。

- [Snort を適用 (Snort Apply)] : Snort 関連ポリシーから障害または応答が発生すると、メッセージがこのセクションに表示されます。通常、このセクションは空です。
- [CLI を適用 (CLI Apply)] : このセクションは、Lina プロセスに送信されたコマンドを使用して設定される機能を対象にしています。
- [インフラストラクチャメッセージ (Infrastructure Messages)] : このセクションには、さまざまな導入モジュールのステータスが表示されます。

[CLI を適用 (CLI Apply)] セクションでは、展開トランスクリプトには、デバイスに送信されたコマンド、およびデバイスから返された応答が含まれます。これらの応答は、通知メッセージやエラーメッセージの場合があります。失敗した展開では、コマンドを含むエラーを示すメッセージを探します。これらのエラーを調べることは、FlexConfig ポリシーを使用してカスタマイズされた機能を設定している場合に特に有用になる場合があります。これらのエラーは、コマンドを設定しようとしている FlexConfig オブジェクトのスク립トを修正するのに役立つ場合があります。

(注) 管理対象機能に送信されるコマンドと、FlexConfig ポリシーから生成されるコマンドとの間のトランスクリプトには違いはありません。

たとえば、次のシーケンスは、論理名が `outside` の `GigabitEthernet0/0` を設定するコマンドを `Management Center` が送信したことを示しています。デバイスは、自動的にセキュリティレベルを `0` に設定したことを応答しました。`Threat Defense` は、何に対してもセキュリティレベルを使用しません。

```
===== CLI APPLY =====  
  
FMC >> interface GigabitEthernet0/0  
FMC >> nameif outside  
FTDv 192.168.0.152 >> [info] : INFO: Security level for "outside" set to 0 by default.
```

アップグレードメッセージの表示

展開メッセージを表示するには、管理者ユーザーであるか、[更新 (Updates)] 権限が必要です。

手順

ステップ 1 [Notification (通告)] をクリックして、メッセージセンターを表示します。

ステップ 2 [アップグレード (Upgrades)] をクリックします。

ステップ 3 次を実行できます。

- 現在のすべてのアップグレードタスクを表示するには、[合計 (Total)] をクリックします。
- 特定のステータスを持つメッセージのみを表示するには、そのステータスの値をクリックします。
- アップグレードタスクの詳細を表示するには、[デバイスの管理 (Device Management)] をクリックします。

正常性メッセージの表示

展開メッセージを表示するには、管理者ユーザーであるか、[正常性 (Health)] 権限が必要です。

手順

ステップ1 [Notification (通告)] をクリックして、メッセージセンターを表示します。

ステップ2 [正常性 (Health)] をクリックします。

ステップ3 次の選択肢があります。

- 現在のすべての正常性ステータスを表示するには、[合計 (total)] をクリックします。シビラティ (重大度) の内訳 (つまり、警告、クリティカル、およびエラー) も表示されません。
- 任意のステータスに関するメッセージのみを表示するには、そのステータスの値をクリックします。
- メッセージが最も最近更新された時刻を表示するには、そのメッセージの相対時間インジケータ (たとえば [3日前 (3 day(s) ago)]) の上にカーソルを置きます。
- 特定のメッセージの詳細な正常性ステータス情報を表示するには、メッセージをクリックします。
- [ヘルスマonitoring (Health Monitoring)] ページの完全な正常性ステータスを表示するには、[ヘルスマonitor (Health Monitor)] をクリックします。

関連トピック

[ヘルスマonitoringについて](#)

タスクメッセージの表示

誰もが自分のタスクを表示できます。他のユーザのタスクを表示するには、管理者ユーザであるか、**他のユーザのタスク表示権限**が必要です。

手順

ステップ1 [通告 (Notification)] をクリックして、メッセージセンターを表示します。

ステップ2 [タスク (Tasks)] をクリックします。

ステップ3 次の選択肢があります。

- 現在のすべてのタスクのステータスを表示するには、[合計 (Total)] をクリックします。ステータス (待機中、実行中、再試行中、成功、失敗) に基づいてタスクを表示するには、それらをクリックします。
- 任意のステータスのタスクに関するメッセージのみを表示するには、そのステータスの値をクリックします。

(注) 停止したタスクのメッセージは、タスクのステータスメッセージの合計リストにのみ表示されます。停止したタスクではフィルタリングできません。

- メッセージが最も最近更新された時刻を表示するには、そのメッセージの相対時間インジケータ（たとえば [3 日前 (3 day(s) ago)]）の上にカーソルを置きます。
- タスクに関する詳細を表示するには、メッセージ内のリンクをクリックします。
- さらにタスクのステータス メッセージが表示可能な場合は、メッセージリストの下部にある [さらにメッセージを取得する (Fetch more messages)] をクリックして取得します。

タスクメッセージの管理

誰もが自分のタスクを表示できます。他のユーザのタスクを表示するには、管理者ユーザであるか、**他のユーザのタスク表示権限**が必要です。

手順

ステップ 1 [システムステータス (System Status)] アイコンをクリックして、メッセージセンターを表示します。

ステップ 2 [タスク (Tasks)] をクリックします。

ステップ 3 次の選択肢があります。

- さらにタスクのステータス メッセージが表示可能な場合は、メッセージリストの下部にある [さらにメッセージを取得する (Fetch more messages)] をクリックして取得します。
- 完了したタスク（ステータスが停止、成功、または失敗のタスク）に関する 1 つのメッセージを削除するには、メッセージの横にある [削除 (Remove)] () をクリックします。
- すべての完了しているタスク（ステータスが停止、成功、または失敗のタスク）に関するメッセージをすべて削除するには、[総数 (total)] でメッセージをフィルタリングして、[すべての完了タスクの削除 (Remove all completed tasks)] をクリックします。
- すべての正常に完了したタスクに関するメッセージをすべて削除するには、[成功 (success)] でメッセージをフィルタリングして、[すべての成功タスクの削除 (Remove all successful tasks)] をクリックします。
- すべての失敗したタスクに関するメッセージをすべて削除するには、[失敗 (failure)] でメッセージをフィルタリングして、[すべての失敗タスクの削除 (Remove all failed tasks)] をクリックします。

ヘルスマニターアラートのメモリ使用率しきい値

メモリ使用率ヘルスマジュールは、アプライアンス上のメモリ使用率をモジュールに設定された制限と比較し、使用率がそのレベルを超えるとアラートを出します。このモジュールは、管理対象デバイスおよび Management Center 自体のデータをモニターします。

メモリ使用率の2つの設定可能なしきい値である「クリティカル」と「警告」は、使用されるメモリのパーセンテージとして設定できます。これらのしきい値を超えると、指定された重大度レベルでヘルスアラームが生成されます。ただし、ヘルスアラームシステムはこれらのしきい値を正確に計算しません。

高メモリデバイスでは、低メモリフットプリントデバイスよりも、特定のプロセスがシステムメモリ全体の大きな割合を使用することが予想されます。この設計では、物理メモリをできるだけ多く使用し、補助的なプロセス用に小さい値のメモリを解放します。

たとえば、32 GB のメモリを搭載したデバイスと 4 GB のメモリを搭載したデバイスを比較します。補助的なプロセスのために解放される 5% のメモリは、32 GB のメモリを搭載したデバイスでは 1.6 GB、4 GB のメモリを搭載したデバイスでは 200 MB であり、前者の方がはるかに大きな値になります。

特定のプロセスによるシステムメモリの使用率が高いことを考慮して、Management Center は、合計物理メモリと合計スワップメモリの両方を含めて合計メモリを計算します。そのため、ユーザーが設定するしきい値入力に対して適用されるメモリしきい値により、イベントの「値」列が、超過しきい値を特定するために入力された値と一致しないようなヘルスイベントが発生する可能性があります。

バージョン 7.4.1 以降、メモリ使用率正常性モジュールは、使用可能な空きメモリ、使用可能なスワップメモリ、およびバッファキャッシュを考慮してメモリ使用率を計算します。メモリ使用率正常性アラートの早すぎる生成を回避するために、警告およびクリティカルアラームのしきい値である 88% と 90% を超えないようにすることをお勧めします。

次の表は、搭載するシステムメモリに応じた、ユーザー入力のしきい値と適用されるしきい値の例を示しています。



- (注) この表の値は一例です。この情報を使用して、ここに示されている搭載 RAM と一致しないデバイスのしきい値を推定することができます。また、より正確なしきい値の計算について Cisco TAC に問い合わせることもできます。

表 1: 搭載する RAM に基づくメモリ使用率しきい値

ユーザー入力しきい値	搭載するメモリ (RAM) ごとの適用しきい値			
	4 GB	6 GB	32 GB	48 GB
10%	10%	34 %	72%	81 %
20 %	20 %	41%	75%	83 %
30%	30%	48 %	78%	85 %
40%	40%	56 %	81 %	88 %
50%	50%	63 %	84 %	90%
60 %	60 %	70%	88 %	92%

ユーザー入力しきい値	搭載するメモリ (RAM) ごとの適用しきい値			
	4 GB	6 GB	32 GB	48 GB
70%	70%	78%	91 %	94%
80%	80%	85 %	94%	96%
90 %	90 %	93%	97%	98%
100 %	100 %	100 %	100 %	100 %



注意 Management Center がクリティカルシステムメモリ状態に達すると、システムは、メモリ使用量の多いプロセスを終了したり、高いメモリ使用率が続く場合には Management Center を再起動する可能性があります。

ディスク使用率とイベントドレインの正常性モニターアラート

Disk Usage 正常性モジュールは、管理対象デバイスのハードドライブとマルウェアストレージパック上のディスク使用率をモジュールに設定された制限と比較し、その使用率がモジュールに設定されたパーセンテージを超えた時点でアラートを出します。また、モジュールしきい値に基づいて、システムが監視対象のディスク使用カテゴリ内のファイルを過剰に削除する場合、または、これらのカテゴリを除くディスク使用率が過剰なレベルに達した場合にもアラートを出します。

このトピックでは、Disk Usage 正常性モジュールによって生成される未処理イベントのドレイン正常性アラートの症状とトラブルシューティングのガイドラインについて説明します。

ディスクマネージャのプロセスは、デバイスのディスク使用率を管理します。ディスクマネージャによってモニターされる各タイプのファイルには、サイロが割り当てられます。システムで使用可能なディスク容量に基づいて、ディスクマネージャは各サイロの最高水準点 (High Water Mark、HWM) と最低水準点 (Low Water Mark、LWM) を計算します。

システムの各部分のディスク使用率の詳細情報 (サイロ、LWM、HWM など) を表示するには、**show disk-manager** コマンドを使用します。

例

次に、ディスクマネージャ情報の例を示します。

```
> show disk-manager
Silo                               Used           Minimum       Maximum
Temporary Files                    0 KB           499.197 MB   1.950 GB
Action Queue Results                0 KB           499.197 MB   1.950 GB
User Identity Events                 0 KB           499.197 MB   1.950 GB
```

UI Caches	4 KB	1.462 GB	2.925 GB
Backups	0 KB	3.900 GB	9.750 GB
Updates	0 KB	5.850 GB	14.625 GB
Other Detection Engine	0 KB	2.925 GB	5.850 GB
Performance Statistics	33 KB	998.395 MB	11.700 GB
Other Events	0 KB	1.950 GB	3.900 GB
IP Reputation & URL Filtering	0 KB	2.437 GB	4.875 GB
Archives & Cores & File Logs	0 KB	3.900 GB	19.500 GB
Unified Low Priority Events	1.329 MB	4.875 GB	24.375 GB
RNA Events	0 KB	3.900 GB	15.600 GB
File Capture	0 KB	9.750 GB	19.500 GB
Unified High Priority Events	0 KB	14.625 GB	34.125 GB
IPS Events	0 KB	11.700 GB	29.250 GB

正常性アラートの形式

Management Center の正常性モニタープロセスが実行されると（5分ごとに1回、または手動実行がトリガーされると）、ディスク使用状況モジュールは `diskmanager.log` ファイルを調べ、該当する条件が満たされると、正常性アラートがトリガーされます。

正常性アラートの構造は、「Drain of unprocessed events from <SILO NAME>」です。

たとえば、「Drain of unprocessed events from Low Priority Events」のようになります。



重要 イベントサイロのみが Drain of unprocessed events from <SILO NAME> 正常性アラートを生成します。このアラートの重大度レベルは常に [重大 (Critical)] です。

アラート以外のその他の症状には、次のものがあります。

- Management Center ユーザーインターフェイスの速度低下
- イベントの喪失

一般的なトラブルシューティング シナリオ

Drain of unprocessed events of <SILO NAME> 正常性アラートは、イベント処理パスのボトルネックが原因で発生します。

これらのディスク使用率アラートに関して、次の3つのボトルネックが存在する可能性があります。

- 過剰なロギング：Threat Defense の EventHandler プロセスがオーバーサブスクライブされています（Snort の書き込みよりも読み取りが遅い）。
- Sftunnel ボトルネック：イベント用インターフェイスが不安定またはオーバーサブスクライブ状態です。
- SFDataCorrerator のボトルネック：Management Center と管理対象デバイス間のデータ伝送チャンネルがオーバーサブスクライブ状態です。

過剰なロギング

このタイプの正常性アラートの最も一般的な原因の1つは、過剰な入力です。 **show disk-manager** コマンドから収集された最低水準点 (LWM) と最高水準点 (HWM) の差は、該当サイロが LWM (新たにドレインされた状態) から HWM 値に移行するまでに使用できる容量を示しています。未処理のイベントのドレインがある場合は、ロギング設定を確認してください。

- ダブルロギングを確認する : Management Center でコリレータ *perfstats* を調査すると、ダブルロギングのシナリオを特定できます。

```
admin@FMC:~$ sudo perfstats -Cq < /var/sf/rna/correlator-stats/now
```

- ACP のロギング設定を確認する : アクセスコントロールポリシー (ACP) のロギング設定を確認します。ロギング設定に接続の「開始」と「終了」の両方が含まれている場合は、イベントの数を減らすために、終了のみをログに記録するように設定を変更します。

[接続のロギングのベストプラクティス](#)に記載されているベストプラクティスに従っていることを確認します。

通信のボトルネック : Sftunnel

Sftunnel は、Management Center と管理対象デバイス間の暗号化通信を担当します。イベントはトンネルを介して Management Center に送信されます。管理対象デバイスと Management Center 間の通信チャネル (sftunnel) の接続性の問題や不安定性は、次の原因が考えられます。

- Sftunnel がダウンしているか、不安定 (フラッピングしている)。

Management Center と管理対象デバイスが、TCP ポート 8305 の管理インターフェイス間で到達可能であることを確認します。

sftunnel プロセスは安定している必要があり、予期せず再起動することがあってはいけません。これを検証するには、**/var/log/message** ファイルを確認し、文字列 **sftunneld** を含むメッセージを検索します。

- Sftunnel がオーバーサブスクライブされている。

正常性モニターからのトレンドデータを確認し、Management Center の管理インターフェイスのオーバーサブスクリプションの兆候を探します。この徴候には、管理トラフィックのスパイクや一定したオーバーサブスクリプションなどがあります。

イベントのセカンダリ管理インターフェイスとして使用します。このインターフェイスを使用するには、Threat Defense CLI で **configure network management-interface** コマンドを使用して、IP アドレスなどのパラメータを設定する必要があります。

通信のボトルネック : SFDataCorrerator

SFDataCorrerator は、Management Center と管理対象デバイス間のデータ伝送を管理します。Management Center では、システムによって作成されたバイナリファイルを分析して、イベント、接続データ、およびネットワークマップを生成します。最初のステップでは、**diskmanager.log** ファイルを調べて、次のような重要な情報を収集します。

- ドレインの頻度。

- 未処理イベントを含むファイルがドレインされた数。
- 未処理イベントによるドレインの発生。

ディスクマネージャプロセスが実行されるたびに、各サイロのエントリが独自のログファイルに生成されます。エントリは、`[ngfw]/var/log/diskmanager.log` 下に存在します。diskmanager.log (CSV形式) から収集された情報は、原因の検索を絞り込むために使用できます。

その他のトラブルシューティング手順：

- コマンド `stats_unified.pl` は、Management Center に送信する必要があるデータが管理対象デバイスにあるかどうかを判断するのに役立ちます。この状態は、管理対象デバイスと Management Center で接続の問題が生じた場合に発生する可能性があります。管理対象デバイスは、ログデータをハードドライブに保存します。

```
admin@FMC:~$ sudo stats_unified.pl
```

- `manage_proc.pl` コマンドは、Management Center 側のコリレータを再設定できます。

```
root@FMC:~# manage_procs.pl
```

Cisco Technical Assistance Center (TAC) に問い合わせる前に

Cisco TACに連絡する前に、次の項目を収集することを強く推奨します。

- 表示される正常性アラートのスクリーンショット。
- Management Center から生成されたトラブルシュートファイル。
- 影響を受ける管理対象デバイスから生成されたトラブルシュートファイル。
問題が最初に検出された日時。
- ポリシーに最近加えられた変更に関する情報（該当する場合）。

[通信のボトルネック：SFDDataCorrerator \(14 ページ\)](#) で説明されている stats_unified.pl コマンドの出力。

デバイス設定履歴ファイルのディスク使用量

[ディスク使用量 (Disk Usage)] 正常性モジュールは、Management Center 上のデバイス設定履歴ファイルのサイズをモニターし、サイズが許容制限を超えると正常性アラートを送信します。デバイス設定履歴ファイルの保存に関する最大許容ディスクサイズは 20 GB です。

Management Center の高可用性展開では、この正常性アラートは、高可用性同期が一時停止されている場合にのみスタンバイ Management Center に表示されます。

デバイス設定履歴ファイルのサイズが許容制限を超えると、Management Center のアップグレード中にアップグレードの準備に失敗する可能性があります。Management Center の高可用性展開では、デバイス設定履歴ファイルのサイズ制限を超えると、高可用性同期速度が低下する可能性があります。

デバイス設定履歴ファイルサイズの正常性アラートを解消するには、**[展開 (Deploy)] > [展開履歴 (Deployment History)] > [展開設定 (Deployment Setting)] > [設定バージョンの設定 (Configuration Version Setting)]** を選択し、**[保持するバージョンの数 (Number of Versions to Retain)]** を減らします。バージョンの数を減らすと、選択したバージョンサイズと一致するように最も古い設定バージョンが削除されます。**[設定バージョンの推定サイズ (Estimated Configuration Version Size)]** は、保持することを選択したバージョンの数に基づいて、Management Center 上の設定履歴ファイルのおおよそのサイズを提供します。推定値を使用してバージョンの数を変更し、設定バージョンのサイズを許容制限未満に減らします。

詳細については、『Cisco Secure Firewall Management Center Device Configuration Guide』の「Set the Number of Configuration Versions」を参照してください。

トラブルシューティング用のヘルス モニター レポート

アプライアンスで問題が発生したときに、問題の診断に役立つように、サポートからトラブルシューティングファイルを提供するように依頼されることがあります。システムは、特定の機能分野を対象とした情報を含むトラブルシューティングファイルと、高度なトラブルシューティングファイル（このファイルはサポートと連携して取得します）を生成することができます。次の表に示すオプションのいずれかを選択して、特定の機能のトラブルシューティングファイルの内容をカスタマイズできます。

一部のオプションは報告対象のデータの点で重複していますが、トラブルシューティングファイルには、オプションの選択に関係なく冗長コピーは含まれません。

表 2: 選択可能なトラブルシューティング オプション

オプション	報告内容
Snort のパフォーマンスと設定 (Snort Performance and Configuration)	アプライアンス上の Snort に関連するデータと構成設定
ハードウェアパフォーマンスとログ (Hardware Performance and Logs)	アプライアンスハードウェアのパフォーマンスに関連するデータとログ
システムの設定、ポリシー、ログ (System Configuration, Policy, and Logs)	アプライアンスの現在のシステム設定に関連する構成設定、データ、およびログ
検知機能の構成、ポリシー、ログ (Detection Configuration, Policy, and Logs)	アプライアンス上の検知機能に関連する構成設定、データ、およびログ
インターフェイスとネットワーク関連データ (Interface and Network Related Data)	アプライアンスのインラインセットとネットワーク設定に関連する構成設定、データ、およびログ
検知、認識、VDB データ、およびログ (Discovery, Awareness, VDB Data, and Logs)	アプライアンス上の現在の検出設定と認識設定に関連する構成設定、データ、およびログ
データおよびログのアップグレード (Upgrade Data and Logs)	アプライアンスの以前のアップグレードに関連するデータおよびログ

オプション	報告内容
All Database Data	トラブルシュートレポートに含まれるすべてのデータベース関連データ
All Log Data	アプライアンス データベースによって収集されたすべてのログ
ネットワーク マップ情報	現在のネットワーク トポロジデータ

特定のシステム機能のトラブルシューティング ファイルの生成

カスタマイズしたトラブルシューティングファイルを生成およびダウンロードして、そのファイルをサポートに送信できます。

始める前に

このタスクを実行するには、管理者ユーザー、メンテナンスユーザー、またはセキュリティアナリストユーザー（読み取り専用）である必要があります。

手順

ステップ 1 [デバイス正常性モニターの表示](#)の手順を実行します。

ステップ 2 システム (⚙️) > [正常性 (Health)] > [モニター (Monitor)] の順に選択し、左側のパネルでデバイスをクリックして、[システムおよびトラブルシューティングの詳細を表示 (View System & Troubleshoot Details)]、[トラブルシューティング ファイルの生成 (Generate Troubleshooting Files)] の順にクリックします。

- (注)
- Management Center Web インターフェイスから Management Center トラブルシューティング ファイルを生成すると、ファイルは Management Center に保存されます。最新のトラブルシューティング ファイルのみが Management Center に保存されることに注意してください。
 - Management Center Web インターフェイスから Threat Defense トラブルシューティング ファイルを生成すると、ファイルは Threat Defense で生成され、Management Center にコピーされます。最新の Threat Defense トラブルシューティング ファイルのみが Management Center に保存されることに注意してください。
 - Management Center と Threat Defense のトラブルシューティング ファイルが CLI から生成されると、トラブルシューティングファイルのすべてのバージョンがそれぞれ Management Center と Threat Defense に保持されます。

ステップ 3 [全データ (All Data)] を選択して生成可能なすべてのトラブルシューティング データを生成することも、個別のボックスをオンにすることもできます。詳細については、[タスクメッセージの表示 \(9 ページ\)](#) を参照してください。

ステップ 4 [生成 (Generate)] をクリックします。

- ステップ5 Message Center でタスク メッセージを表示します。 [タスクメッセージの表示 \(9 ページ\)](#) を参照してください。
- ステップ6 生成されたトラブルシューティング ファイルに対応するタスクを探します。
- ステップ7 アプライアンスがトラブルシューティング ファイルを生成して、タスク ステータスが [完了 (Completed)] に変わったら、[クリックして生成されたファイルを取得 (Click to retrieve generated files)] をクリックします。
- ステップ8 ブラウザのプロンプトに従ってファイルをダウンロードします。(トラブルシューティングファイルは、1 つの .tar.gz ファイルでダウンロードされます)。
- ステップ9 サポートの指示に従って、トラブルシューティング ファイルを Cisco に送信してください。

高度なトラブルシューティング ファイルのダウンロード

トラブルシューティング ファイルをダウンロードできます。

始める前に

このタスクを実行するには、管理者ユーザー、メンテナンスユーザー、またはセキュリティアナリストユーザー（読み取り専用）である必要があります。

手順

-
- ステップ1 アプライアンスの正常性モニターを表示します。、 [デバイス正常性モニターの表示](#) を参照してください。
 - ステップ2 システム (⚙️) > [正常性 (Health)] > [モニター (Monitor)] の順に選択し、左側のパネルでデバイスをクリックして、[システムおよびトラブルシューティングの詳細を表示 (View System & Troubleshoot Details)]、[高度なトラブルシューティング (Advanced Troubleshooting)] の順にクリックします。
 - ステップ3 [ファイルのダウンロード (File Download)] で、サポートから提供されたファイル名を入力します。
 - ステップ4 [ダウンロード (Download)] をクリックします。
 - ステップ5 ブラウザのプロンプトに従ってファイルをダウンロードします。
(注) 管理対象デバイスでは、システムはファイル名の前にデバイス名を付加してファイル名を変更します。
 - ステップ6 サポートの指示に従って、トラブルシューティング ファイルを Cisco に送信してください。
-

一般的なトラブルシューティング

内部電源障害（ハードウェア障害、電源サージなど）や外部電源の障害（コードが外れている）によって、グレースフルでないシャットダウンまたは再起動が発生することがあります。これによってデータが破損することがあります。

接続ベースのトラブルシューティング

接続ベースのトラブルシューティングまたはデバッグにおいて、モジュール間で一貫したデバッグが提供され、特定の接続について適切なログを収集します。また、レベルベースのデバッグを最大7レベルまでサポートし、モジュール間で一貫したログ収集メカニズムを使用できます。接続ベースのデバッグでは、次の機能がサポートされています。

- **Threat Defense** の問題をトラブルシューティングする一般的な接続ベースのデバッグサブシステム
- モジュール間のデバッグメッセージで均一的な形式
- リポート後の永続的なデバッグメッセージ
- 既存の接続に基づくモジュール間のエンドツーエンドのデバッグ
- 進行中の接続のデバッグ



(注) 接続ベースのデバッグは、Firepower 2100 シリーズ デバイスではサポートされていません。

接続のトラブルシューティングの詳細については、[接続のトラブルシューティング \(19 ページ\)](#) を参照してください。

接続のトラブルシューティング

手順

ステップ 1 **debug packet-condition** コマンドを使用して接続を識別するためのフィルタを設定します。

例：

```
Debug packet-condition match tcp 192.168.100.177 255.255.255.255 192.168.102.177  
255.255.255.255
```

ステップ 2 対象モジュールおよび対応するレベルのデバッグを有効にします。**debug packet** コマンドを入力します。

例：

```
Debug packet acl 5
```

ステップ3 次のコマンドを使用して、パケットのデバッグを開始します。

```
debug packet-start
```

ステップ4 データベースからデバッグ メッセージを取得し、次のコマンドを使用してデバッグ メッセージを分析します。

```
show packet-debug
```

ステップ5 次のコマンドを使用して、パケットのデバッグを停止します。

```
debug packet-stop
```

Secure Firewall Threat Defense デバイスの高度なトラブルシューティング

Secure Firewall Threat Defense デバイスでは、パケットトレーサ機能とパケットキャプチャ機能を使って詳細なトラブルシューティング分析が可能です。パケットトレーサを使うと、ファイアウォール管理者はセキュリティアプライアンスに仮想パケットを注入し、入力から出力までのフローを追跡できます。このとき、パケットはフローおよびルーティングルックアップ、ACL、プロトコルインスペクション、NAT、侵入検知に照らして評価されます。このユーティリティは、送信元および宛先のアドレスとプロトコルおよびポート情報を指定することにより、実際のトラフィックをシミュレートできるため、効果的です。パケットキャプチャにはトレースオプションがあり、このオプションを使用すれば、パケットがドロップされたか成功したかの判断を知ることができます。

トラブルシューティング ファイルの詳細については、[高度なトラブルシューティング ファイルのダウンロード \(18 ページ\)](#) を参照してください。

パケット キャプチャの概要

トレースオプションを有効にしたパケットキャプチャ機能では、入力インターフェイスでキャプチャされた実際のパケットをシステム内でトレースできます。トレース情報は後で表示されます。キャプチャしたパケットは、実際のデータパストラフィックであるため、出力インターフェイスでドロップされません。Threat Defense デバイスのパケットキャプチャは、データパケットのトラブルシューティングおよび分析をサポートします。

パケットをキャプチャすると、Snort がパケットで有効になっているトレースフラグを検出します。Snortは、パケットが通過するトレーサエレメントを書き込みます。パケットキャプチャの結果、Snort は次のいずれかの判定結果を出します。

表 3: Snort の判定

判定	説明
成功 (Pass)	分析されたパケットを許可します。
ブロック (Block)	転送されないパケット。
置換 (Replace)	変更されたパケット。
許可フロー (AllowFlow)	インスペクションなしで転送されるフロー。
ブロックフロー (BlockFlow)	フローがブロックされました。
無視	フローがブロックされました。パッシブインターフェイスでフローがブロックされているセッションでのみ発生します。
再試行	フローが停止し、enamelware または URL カテゴリ/レピュテーションクエリを待機しています。タイムアウトが発生した場合、処理は続行され、結果は不明になります。enamelware の場合、ファイルは許可されます。URL カテゴリ/レピュテーションの場合、AC ルールルックアップは未分類の不明なレピュテーションで続行されます。

Snort の判定に基づいて、パケットはドロップまたは許可されます。たとえば、Snort の判定が [ブロックフロー (BlockFlow)] である場合、パケットはドロップされ、セッション内の後続のパケットは Snort に到達する前にドロップされます。Snort の判定が [ブロック (Block)] または [ブロックフロー (BlockFlow)] の場合、[ドロップ理由 (Drop Reason)] は次のいずれかになります。

表 4: ドロップ理由

ブロックまたはフローブロックの実行元	原因
Snort	Snort がパケットを処理できません。たとえば、パケットが破損しているか、無効な形式であるため、Snort がパケットを復号化できません。
前処理されたアプリケーション ID	アプリケーション ID モジュール/前処理されたアプリケーション ID は、それ自体はパケットをブロックしません。ただし、これは、アプリケーション ID 検出が原因で他のモジュール (ファイアウォールなど) がブロッキングルールに一致することを示している可能性があります。

ブロックまたはフローブロックの実行元	原因
前処理された SSL	SSLポリシーにトラフィックと一致するブロック/リセットルールがあります。
ファイアウォール	ファイアウォールポリシーにトラフィックと一致するブロック/リセットルールがあります。
前処理されたキャプティブポータル	トラフィックと一致する、ID ポリシーを使用するブロック/リセットルールがあります。
前処理されたセーフサーチ	トラフィックと一致する、ファイアウォールポリシーのセーフサーチ機能を使用するブロック/リセットルールがあります。
前処理された SI	AC ポリシーの [セキュリティインテリジェンス (Security Intelligence)] タブに、トラフィックをブロックするブロック/リセットルールがあります (DNS または URL SI ルールなど)。
前処理された filterer	AC ポリシーの [filterer] タブに、トラフィックと一致するブロック/リセットルールがあります。
前処理されたストリーム	侵入ルールのブロッキング/リセットストリーム接続があります (TCP 正規化エラー時のブロッキングなど)。
前処理されたセッション	このセッションは他のモジュールによってすでにブロックされているため、前処理されたセッションが同じセッションの以降のパケットをブロックしています。
前処理されたフラグメンテーション	データの以前のフラグメントがブロックされているため、ブロックしています。
前処理された snort 応答	たとえば、特定の HTTP トラフィックで応答ページを送信する、react snort ルールがあります。
前処理された snort 応答	条件に一致するパケットに、カスタム応答を送信する snort ルールがあります。
前処理されたレピュテーション	パケットがレピュテーションルール (特定の IP アドレスのブロッキングなど) に一致しています。
前処理された x-Link2State	SMTP で検出されたバッファオーバーフローの脆弱性によるブロッキング。

ブロックまたはフローブロックの実行元	原因
前処理された back orifice	back orifice データの検出によるブロッキング。
前処理された SMB	SMB トラフィックをブロックする snort ルールがあります。
前処理されたファイルプロセス	ファイルをブロックするファイルポリシーがあります (enamelware ブロッキングなど)。
前処理された IPS	IPS を使用する snort ルールがあります (レートフィルタリングなど)。

パケットキャプチャ機能を使用すると、システムメモリに保存されているパケットをキャプチャしてダウンロードできます。ただし、メモリの制約により、バッファサイズは 32 MB に制限されます。大量のパケットキャプチャを処理できるシステムはすぐに最大バッファサイズを超過するため、パケットキャプチャの制限を増やす必要があります。これを行うには、セカンダリメモリを使用します (ファイルを作成してキャプチャデータを書き込む)。サポートされている最大ファイルサイズは 10 GB です。

file-size を設定すると、キャプチャされたデータがファイルに保存され、キャプチャ名 **recapture** に基づいてファイル名が割り当てられます。

ファイルサイズ オプションは、32 MB 以上のサイズ制限のパケットをキャプチャする必要がある場合に使用されます。

詳細については、[Cisco Secure Firewall Threat Defense コマンドリファレンス](#)を参照してください。

キャプチャトレースの使用

パケットキャプチャは、定義された基準に基づいてデバイスの指定されたインターフェイスを通過するネットワークトラフィックのライブスナップショットを提供するユーティリティです。このプロセスは、一時停止していない限り、または割り当てられたメモリが使い果たされていない限り、パケットのキャプチャを続行します。

パケットキャプチャデータには、パケットの処理中にシステムが行う決定とアクションに関する Snort とプリプロセッサからの情報が含まれています。一度に複数のパケットキャプチャを実行できます。キャプチャの変更、削除、クリア、保存を実行するようにシステムを設定できます。



- (注) パケットデータのキャプチャには、パケットのコピーが必要です。この操作によって、パケットの処理中に遅延が生じる可能性があります。また、パケットのスループットが低下する可能性もあります。特定のデータトラフィックをキャプチャするためにパケットフィルタを使用することをお勧めします。

始める前に

Secure Firewall Threat Defense デバイスでパケットキャプチャツールを使用するには、管理者またはメンテナンスユーザーである必要があります。

手順

ステップ 1 Management Center で、[デバイス (Devices)] > [パケットキャプチャ (Packet Capture)] を選択します。

ステップ 2 デバイスを選択します。

ステップ 3 [キャプチャの追加 (Add Capture)] をクリックします。

ステップ 4 トレースのキャプチャの [名前 (Name)] を入力します。

ステップ 5 トレースのキャプチャの [インターフェイス (Interface)] を選択します。

ステップ 6 以下の [一致基準 (Match Criteria)] の詳細を指定します。

- a) [プロトコル (Protocol)] を選択します。
- b) [送信元ホスト (Source Host)] の IP アドレスを入力します。
- c) [宛先ホスト (Destination Host)] の IP アドレスを入力します。
- d) (オプション) [SGT 番号 (SGT number)] チェックボックスをオンにし、セキュリティグループタグ (SGT) を入力します。

ステップ 7 以下の [バッファ (Buffer)] の詳細を指定します。

- a) (オプション) 最大 [パケット サイズ (Packet Size)] を入力します。
- b) (オプション) 最小 [バッファ サイズ (Buffer Size)] を入力します。
- c) 中断せずにトラフィックをキャプチャしたい場合は、[連続キャプチャ (Continuous Capture)] を選択し、最大バッファ サイズに到達したらキャプチャを停止したい場合は、[いっぱいになったら停止 (Stop when full)] を選択します。

(注) [連続キャプチャ (Continues Capture)] がオンになっている場合、割り当てられたメモリがいっぱいになると、メモリ内の最も古いキャプチャ済みパケットが、新しくキャプチャされたパケットで上書きされます。

- d) 各パケットの詳細をキャプチャする場合は、[トレース (Trace)] チェックボックスをオンにします。
- e) [トレース数 (Trace Count)] フィールドに値を入力します。デフォルト値は 128 です。1 ~ 1000 の範囲で値を入力できます。

ステップ 8 [保存 (Save)] をクリックします。

パケットキャプチャ画面に、パケットキャプチャの詳細とそのステータスが表示されます。パケットキャプチャページを自動更新するには、[自動更新の有効化 (Enable Auto Refresh)] チェックボックスをオンにして、自動更新間隔を秒単位で入力します。

パケットキャプチャでは、次の操作を実行できます。

- [編集 (Edit)] (✎) : キャプチャ基準を変更できます。

- [削除 (Delete)] () : パケットキャプチャとキャプチャされたパケットを削除できます。
- [クリア (Clear)] () : 1つのパケットキャプチャから、キャプチャされたすべてのパケットを消去できます。既存のすべてのパケットキャプチャから、キャプチャされたパケットを消去するには、[すべてのパケットをクリア (Clear All Packets)]をクリックします。
- [一時停止 (Pause)] () : パケットのキャプチャを一時的に停止できます。
- [保存 (Save)] () : キャプチャされたパケットのコピーを ASCII または PCAP 形式でローカルマシンに保存できます。必要な形式オプションを選択し、[保存 (Save)]をクリックします。保存されたパケットキャプチャがローカルマシンにダウンロードされません。
- キャプチャされているパケットの詳細を表示するには、必要なキャプチャ行をクリックします。

パケットトレーサの概要

パケットトレーサツールを使用すると、送信元および宛先のアドレスとプロトコルの特性によってパケットをモデル化することにより、ポリシー設定をテストできます。トレースでは、ポリシールックアップが実行され、設定済みのアクセスルール、NAT、ルーティング、アクセスポリシー、レート制限ポリシーに基づいてパケットが許可されるか拒否されるかが確認されます。パケットフローは、インターフェイス、送信元アドレス、宛先アドレス、ポート、プロトコルに基づいてシミュレートされます。この方式でパケットをテストすることによって、ポリシーの有効性を確認し、必要に応じて、許可または拒否するトラフィックのタイプが処理されるかどうかをテストできます。

設定の確認に加えて、トレーサを使用して、アクセスを許可すべきパケットが拒否されるなどの予期せぬ動作をデバッグできます。パケットを完全にシミュレートするために、パケットトレーサはデータパス（低速パスモジュールと高速パスモジュール）をトレースします。当初は、処理が、セッション単位またはパケット単位のトランザクションとして行われていました。ファイアウォールがセッション単位またはパケット単位でパケットを処理する際は、パケットトレーサツールと「トレースによるキャプチャ」機能により、パケット単位でトレースデータがログに記録されます。

PCAP ファイル

PCAP ファイルを使用してパケットトレーサを開始できます。これにより、完全なフローが実現されます。現時点では、単一のTCP/UDPベースのフローおよび最大100パケットでのPCAPのみがサポートされています。パケットトレーサツールは、PCAP ファイルを読み取り、クライアントとサーバーのリプレイエンティティの状態を初期化します。ツールは、後続の処理と表示のためにPCAP内の各パケットのトレース出力を収集して保存することで、同期方式でパケットのリプレイを開始します。

PCAP リプレイ

パケットリプレイは、PCAP ファイル内のパケットのシーケンスによって実行されます。リプレイアクティビティへの干渉があると、リプレイアクティビティが中断され、リプレイが終了します。指定された入力インターフェイスおよび出力インターフェイスにおける PCAP のすべてのパケットについてトレース出力が生成されるため、フロー評価の完全なコンテキストが提供されます。

PCAP リプレイは、リプレイ中にパケットを動的に変更する一部の機能（IPsec、VPN、SSL、HTTP 復号、NAT など）ではサポートされません。

パケット トレーサの使用

Secure Firewall Threat Defense デバイスでパケットトレーサを使用するには、管理者またはメンテナンスマスターである必要があります。

手順

-
- ステップ 1** Management Center で、**デバイス > パケットトレーサ** を選択します。
- ステップ 2** [デバイスの選択 (Select Device)] ドロップダウンリストから、トレースを実行するデバイスを選択します。
- ステップ 3** [入力インターフェイス (Ingress Interface)] ドロップダウンリストから、パケットトレーサ用の入力インターフェイスを選択します。
- (注) [VTI] を選択しないでください。パケットトレーサでは、入力インターフェイスとしての VTI はサポートされていません。
- ステップ 4** パケットトレーサで PCAP リプレイを使用するには、次の手順を実行します。
- [PCAPファイルの選択 (Select a PCAP File)] をクリックします。
 - 新しい PCAP ファイルをアップロードするには、[PCAPファイルのアップロード (Upload aPCAP file)] をクリックします。最近アップロードしたファイルを再利用するには、リストからファイルをクリックします。
- (注) .pcap および .pcapng ファイル形式のみがサポートされています。PCAP ファイルには、最大 100 パケットの TCP/UDP ベースのフローを 1 つだけ含めることができます。PCAP ファイル名 (ファイル形式を含む) の最大文字数は 64 文字です。
- [PCAPのアップロード (Upload PCAP)] ボックスで、PCAP ファイルをドラッグするか、ボックスをクリックしてファイルを参照およびアップロードすることができます。ファイルを選択すると、アップロードプロセスが自動的に開始されます。
 - この [ステップ 13](#) に進みます。
- ステップ 5** トレースパラメータを定義するには、[プロトコル (Protocol)] ドロップダウンメニューからトレースのパケットタイプを選択し、プロトコル特性を指定します。
- [ICMP]: ICMP タイプ、ICMP コード (0 ~ 255)、およびオプションで ICMP 識別子を入力します。
 - [TCP/UDP/SCTP]: 送信元および宛先のポート番号を入力します。

- [GRE/IPIP] : プロトコル番号 (0 ~ 255) を入力します。
- [ESP] : 送信元の SPI 値 (0 ~ 4294967295) を入力します。
- [RAWIP] : プロトコル番号 (0 ~ 255) を入力します。

ステップ 6 パケットトレースの [送信元タイプ (Source Type)] を選択し、送信元 IP アドレスを入力します。

送信元と宛先のタイプとして、IPv4、IPv6、完全修飾ドメイン名 (FQDN) を選択できます。Cisco TrustSec を使用する場合、IPv4 または IPv6 アドレスと FQDN を指定できます。

ステップ 7 パケット トレースの [送信元ポート (Source Port)] を選択します。

ステップ 8 パケット トレースの [宛先 (Destination)] タイプを選択し、宛先 IP アドレスを入力します。
宛先タイプのオプションは、選択した送信元タイプによって異なります。

ステップ 9 パケット トレースの [宛先ポート (Destination Port)] を選択します。

ステップ 10 オプションで、セキュリティ グループ タグ (SGT) 値がレイヤ 2 CMD ヘッダー (TrustSec) に組み込まれているパケットをトレースする場合、有効な [SGT 番号 (SGT number)] を入力します。

ステップ 11 パケット トレーサで親インターフェイスに入力する (後でサブインターフェイスにリダイレクトされる) 場合は、[VLAN ID] を入力します。

インターフェイスタイプはすべてサブインターフェイスで設定するため、これはサブインターフェイスを使用しない場合だけのオプションです。

ステップ 12 パケット トレースの [宛先 MAC アドレス (Destination MAC Address)] を指定します。

Secure Firewall Threat Defense デバイスをトランスペアレント ファイアウォール モードで実行していて、入力インターフェイスが VTEP であるとき、[VLAN ID] に値を入力する場合は、[宛先 MAC アドレス (Destination MAC Address)] は必須になります。一方、インターフェイスがブリッジグループのメンバーであるとき、[VLAN ID] に値を入力する場合は [宛先 MAC アドレス (Destination MAC Address)] はオプションですが、[VLAN ID] に値を入力しない場合は必須になります。

Secure Firewall Threat Defense をルーテッドファイアウォール モードで実行しているときに、入力インターフェイスがブリッジグループのメンバーである場合、[VLAN ID] と [宛先 MAC アドレス (Destination MAC Address)] はオプションになります。

ステップ 13 (任意) パケットトレーサで、シミュレートされたパケットのセキュリティチェックを無視する場合は、[シミュレートされたパケットのすべてのセキュリティチェックをバイパスする (Bypass all security check for Simulated packet)] をクリックします。これにより、パケットトレーサは、これを設定しないとシステムを通過するときにドロップされるパケットのトレースを継続できるようになります。

ステップ 14 (任意) デバイスから出力インターフェイスを介してパケットを送信できるようにするには、[シミュレートされたパケットがデバイスから送信できるようにする (Allow Simulated packet to transmit from device)] をクリックします。

ステップ 15 (任意) パケットトレーサで、インジェクトされたパケットを IPsec/SSL VPN で復号されたパケットと見なすようにするには、[シミュレートされたパケットをIPsec/SSL VPN復号として扱う (Treat simulated packet as IPsec/SSL VPN decrypt)] をクリックします。

ステップ 16 [トレース (Trace)] をクリックします。

[トレース結果 (Trace Result)] には、PCAP パケットがシステムを通過した各フェーズの結果が表示されます。個々のパケットのトレース結果を表示するには、そのパケットをクリックします。次を実行できます。

- トレース結果をクリップボードにコピー (📄) します。
- 表示される結果を展開したり折りたたんだり (☑) します。
- トレース結果画面を最大化 (⌕) します。

要した処理能力の測定に役立つ経過時間情報が、フェーズごとに表示されます。入力インターフェイスから出力インターフェイスへのパケットフロー全体にかかった合計時間も、結果セクションに表示されます。

[トレース履歴 (Trace History)] ペインには、PCAP トレースごとに保存されたトレースの詳細が表示されます。最大100のパケットトレースを保存できます。保存されたトレースを選択して、パケットトレース アクティビティを再度実行できます。次を実行できます。

- 任意のトレースパラメータの使用してトレースを検索します。
- ボタンを使用して、履歴へのトレースの保存を無効にします。
- 特定のトレース結果を削除します。
- すべてのトレースをクリアします。

Web インターフェイスから Threat Defense 診断 CLI を使用する方法

Management Center から選択した Threat Defense 診断 CLI コマンドを実行できます。コマンド **ping** (**ping system** を除く)、**traceroute**、および一部の **show** コマンドは、通常の CLI ではなく診断 CLI で実行されます。

show コマンドを実行したときに、「Unable to execute the command properly. Please see logs for more details」(コマンドを正しく実行できません。詳細については、ログを参照してください) というメッセージが表示される場合は、そのコマンドが診断 CLI で無効であることを意味します。たとえば、**show access-list** は機能しますが、**show access-control-policy** と入力すると、このメッセージが表示されます。非診断コマンドを使用するには、SSH を使用して Management Center の外部のデバイスにログインします。

Threat Defense CLI の詳細については、[Cisco Secure Firewall Threat Defense コマンドリファレンス](#)を参照してください。

始める前に

- 診断 CLI を使用するには、管理者、メンテナンス、またはセキュリティアナリストである必要があります。
- 診断 CLI の目的は、デバイスのトラブルシューティングに役立ついくつかのコマンドをすばやく使用できるようにすることです。すべてのコマンドにアクセスするには、デバイスとの SSH セッションを直接開きます。
- Management Center 高可用性を使用する展開では、診断 CLI は、アクティブ Management Center でのみ使用できます。

手順

ステップ 1 [デバイス (Devices)] > [脅威対策 CLI (Threat Defense CLI)] を選択します。

また、デバイスの正常性モニター (システム (⚙️) > [正常性 (Health)] > [モニター (Monitor)]) から CLI ツールにアクセスすることもできます。そこから、デバイスを選択し、[システムとトラブルシューティングの詳細を表示 (View System and Troubleshoot Details)] リンクをクリックし、[高度なトラブルシューティング (Advanced Troubleshooting)] をクリックして、そのページで [Threat Defense CLI] をクリックします。

ステップ 2 [デバイス (Device)] ドロップダウンリストから、診断コマンドを実行するデバイスを選択します。

ステップ 3 [コマンド (Command)] ドロップダウンリストから、実行するコマンドを選択します。

ステップ 4 [パラメータ (Parameters)] フィールドにコマンドパラメータを入力します。

有効なパラメータについては、[Cisco Secure Firewall Threat Defense コマンドリファレンス](#)を参照してください。

たとえば、**show access-list** コマンドを実行するには、[コマンド (Command)] ドロップダウンリストから **show** を選択し、[パラメータ (Parameters)] フィールドに **access-list** と入力します。

(注) [パラメータ (Parameters)] フィールドにコマンド全体を入力しないでください。関連するキーワードのみを入力してください。

ステップ 5 [実行 (Execute)] をクリックして、コマンド出力を表示します。

「Unable to execute the command properly. Please see logs for more details.」 (コマンドを正しく実行できません。詳細については、ログを参照してください) というメッセージが表示される場合は、パラメータをよく確認してください。構文エラーがある可能性があります。

このメッセージは、実行しようとしているコマンドが診断 CLI (**system support diagnostic-cli** コマンドを使用してデバイスからアクセスした) のコンテキスト内で有効なコマンドではないことを意味する場合があります。これらのコマンドを使用するには、SSH を使用してデバイスにログインします。

機能固有のトラブルシューティング

機能固有のトラブルシューティングのヒントやテクニックについては、次の表を参照してください。

表 5: 機能固有のトラブルシューティング トピック

機能	関連するトラブルシューティング情報
アプリケーション制御	Cisco Secure Firewall Management Center デバイス構成ガイドの「Best Practices for Application Control」
LDAP 外部認証	LDAP 認証接続のトラブルシューティング
ライセンスング	スマート ライセンスのトラブルシューティング 特定のライセンスの予約のトラブルシューティング
Management Center ハイ アベイラビリティ	Management Center のハイ アベイラビリティのトラブルシューティング
ユーザ ルール条件	Cisco Secure Firewall Management Center デバイス構成ガイドの「Troubleshoot User Control」
ユーザ アイデンティティ ソース	ISE/ISE-PIC、TS エージェントアイデンティティ ソース、キャプティブ ポータルアイデンティティ ソース、およびリモートアクセス VPN アイデンティティソースに関するトラブルシューティング情報については、 Cisco Secure Firewall Management Center デバイス構成ガイド の対応する項を参照してください。 LDAP 認証接続のトラブルシューティング
URL フィルタリング	Cisco Secure Firewall Management Center デバイス構成ガイドの「Troubleshoot URL Filtering」
レルムとユーザデータのダウンロード	Cisco Secure Firewall Management Center デバイス構成ガイドの「Troubleshoot Realms and User Downloads」
ネットワーク検出	Cisco Secure Firewall Management Center デバイス構成ガイドの「Troubleshooting Your Network Discovery Strategy」
カスタムセキュリティ グループ タグ (SGT) のルール条件	Cisco Secure Firewall Management Center デバイス構成ガイドの「Custom SGT Rule Conditions」
SSL ルール	Cisco Secure Firewall Device Manager Configuration Guide の SSL ルールに関する章
Cisco Threat Intelligence Director (TID)	Cisco Secure Firewall Management Center デバイス構成ガイドの「Troubleshoot Secure Firewall Threat Intelligence Director」

機能	関連するトラブルシューティング情報
Secure Firewall Threat Defense syslog	Cisco Secure Firewall Management Center デバイス構成ガイド の「 <i>About Configuring Syslog</i> 」
侵入パフォーマンス統計	Cisco Secure Firewall Management Center デバイス構成ガイド の「 <i>Intrusion Performance Statistic Logging Configuration</i> 」
接続ベースのトラブルシューティング	接続ベースのトラブルシューティング (19 ページ)

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。