正常性

次のトピックでは、Firepower システムでヘルス モニタリングを使用する方法について説明します。

ヘルスモニタリングの要件と前提条件

モデルのサポート

いずれか（Any）

サポートされるドメイン

任意

ユーザの役割

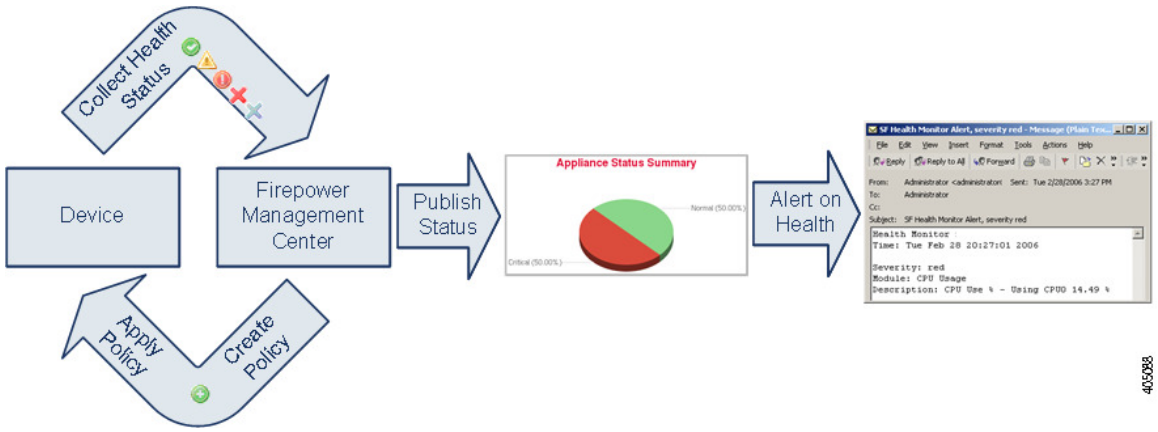
管理者

メンテナンス ユーザー

ヘルス モニタリングについて

Firewall Management Center の正常性モニターでは、さまざまな正常性インジケータを追跡して、システムのハードウェアとソフトウェアが正常に動作することを確認します。正常性モニターを使用して、展開全体の重要な機能のステータスを確認できます。

アラート用に正常性モジュールを実行する頻度を設定できます。Firewall Management Center は、時系列データ収集もサポートしています。デバイスとその正常性モジュールで時系列データを収集する頻度を設定できます。デフォルトでは、デバイスモニターは、いくつかの事前定義されたヘルスモニターダッシュボードでこれらのメトリックを報告します。メトリックデータは分析のために収集されるため、アラートは関連付けられません。



ヘルスモニタを使用すれば、正常性ポリシーとも呼ばれるテストのコレクションを作成し、正常性ポリシーを1つ以上のアプライアンスに適用できます。正常性モジュールとも呼ばれるテストは、指定された基準に照らしてテストするスクリプトです。テストを有効または無効にするか、テスト設定を変更することによって、正常性ポリシーを変更したり、不要になった正常性ポリシーを削除したりできます。アプライアンスを除外することによって、選択したアプライアンスからのメッセージを抑制することもできます。

ヘルスモニタリングシステムは、設定された間隔で正常性ポリシーのテストを実行します。すべてのテストを実行することも、オンデマンドで特定のテストを実行することもできます。ヘルス モニターは設定されたテスト条件に基づいてヘルス イベントを収集します。

（注） すべてのアプライアンスはハードウェアアラームのヘルスモジュール経由でハードウェアのステータスを自動的に報告します。また、Firewall Management Center はデフォルトの正常性ポリシーで設定されているモジュールを使用して自動的にステータスを報告します。アプライアンス ハートビートなどの一部の正常性モジュールは、Firewall Management Center 上で実行され Firewall Management Center の管理対象デバイスのステータスを報告します。正常性モジュールが管理対象デバイスのステータスを提供するには、すべての正常性ポリシーがデバイスに展開されている必要があります。

正常性モニターを使用して、システム全体および特定のアプライアンスの正常性ステータス情報にアクセスできます。マルチドメイン展開では、リーフ ドメインとその親ドメインの両方でデバイスのヘルス ステータスの概要を表示できます。

[正常性ステータス（Health Status）] ページの六角形のチャートとステータ ステーブルにより、Firewall Management Center を含むネットワーク上のすべてのアプライアンスのステータスに関する視覚的なサマリーが提供されます。個々のアプライアンスのヘルス モニタを使用すれば、特定のアプライアンスのヘルス詳細にドリルダウンできます。

完全にカスタマイズ可能なイベント ビューを使用すれば、ヘルス モニタによって収集されたヘルス ステータス イベントを迅速かつ容易に分析できます。このイベント ビューでは、イベントデータを検索して表示したり、調査中のイベントに関係する他の情報にアクセスしたりできます。たとえば、特定のパーセンテージの CPU 使用率の全記録を表示する場合は、CPU 使用率モジュールを検索して、パーセンテージ値を入力できます。

ヘルス イベントに対応した電子メール、SNMP、または syslog アラートを設定することもできます。ヘルス アラートは、標準アラートとヘルス ステータス レベルを関連付けたものです。たとえば、アプライアンスでハードウェアの過負荷による障害が発生することが絶対にない状態を確保するために、電子メールアラートをセットアップできます。その後で、CPU、ディスク、またはメモリの使用率がそのアプライアンスに適用される正常性ポリシーで設定された警告レベルに達するたびに電子メールアラートがトリガーされる正常性アラートを作成できます。アラートしきい値を、受け取る反復アラートの数が最小になるように設定できます。

（注） ヘルスモニタリングでは、正常性イベントの発生から正常性アラートが生成されるまでに 5 ～ 6 分かかることがあります。

サポートから依頼された場合に、アプライアンスのトラブルシューティング ファイルを作成することもできます。

管理者ユーザーロール特権を持つユーザーのみがシステム正常性データにアクセスできます。

高可用性ペア

バージョン 6.7 以降を実行している Firewall Management Center 高可用性展開では、アクティブ Firewall Management Center が、REST API を使用して詳細なメトリックベースの情報を表示する正常性モニターページを作成します。スタンバイ Firewall Management Center は、アラート情報を表示し、円グラフとステータステーブルを使用して、ネットワーク上のすべてのアプライアンスのステータスに関する視覚的なサマリーを提供する正常性モニターページを作成します。スタンバイ Firewall Management Center は、メトリックベースの情報を表示しません。

ヘルス モジュール

ヘルス モジュールまたはヘルス テストは、正常性ポリシーに指定した条件でテストします。

正常性モジュールには、アラートとメトリックの 2 つのタイプがあります。アラート モジュール（レガシー モジュールと呼ばれることもあります）は、システム インフラストラクチャを

監視し、ヘルス ステータスのみを報告します。これらのモニタ対象システムの正常性ポリシーで指定された条件が満たされると、これらのモジュールは正常性アラートを生成します。メトリックモジュール（テレグラフ モジュールと呼ばれることもあります）が収集する統計情報（時系列データと呼ばれることもあります）は、ヘルス モニタリング ダッシュボードに表示できます。優先正常性メトリックを使用してカスタムダッシュボードを作成し、統計をモニターしたり、アプライアンスの正常性の問題をトラブルシューティングすることができます。

表 *1*: デバイスヘルスモジュール

モジュール	タイプ	説明
AMP 接続ステータス	メトリック	このモジュールは、最初に接続に成功した後、デバイスが AMP クラウドまたは Cisco AMP Private Cloud に接続できない場合、またはプライベートクラウドがパブリック AMP クラウドに接続できない場合にアラートを出します。デフォルトでは、ディセーブルです。
AMP Threat Grid の接続	メトリック	このモジュールは、デバイスが AMP Threat Grid クラウドに最初は正常に接続でき、その後接続できなくなった場合にアラートを出します。
ASP ドロップ	メトリック	データ プレーンの高速セキュリティ パスによってドロップされた接続をモニターします。 選択したメトリックのアラートを個別に生成するようにこのモジュールを設定できます。モジュールはこれらのメトリックをモニタし、2 つのタイムスタンプの ASP ドロップ カウンタ値の差が指定のしきい値を超えた場合に障害を検出します。
自動アプリケーションバイパス	Alert	バイパスされた検出アプリケーションをモニタします。
証明書のモニタリング	Alert	サービス認証証明書の有効期限に近づいているか、または期限切れになったときに、設定可能なしきい値（日数単位）に基づいてアラートを発行します。このアラートは、期限切れが近づいている証明書を特定し、サービスの中断が発生する前に証明書を更新するために役立ちます。
シャーシ環境ステータス	Alert	ファン速度やシャーシ温度などのシャーシパラメータをモニターします。また、温度の警告しきい値とクリティカルしきい値を設定できます。クリティカルシャーシ温度（摂氏）のデフォルト値は 85 です。警告シャーシ温度（摂氏）のデフォルト値は 75 です。 デフォルトでは、Firepower 1010 の CPU 温度しきい値は `100` であり、Firepower 1010 デバイスの CPU 温度が 100 °C に達すると、このモジュールは高 CPU 温度アラートを生成します。
クラスタ/HA 障害ステータス	Alert	Threat Defense クラスタの場合、ユニットがプライマリに参加、離脱するか、プライマリとして選出されたときにアラートを出します。

モジュール	タイプ	説明
設定のリソース使用率	Alert	展開された設定のサイズに基づき、デバイスがメモリ不足になるリスクがある場合にアラートを出します。 アラートには、設定に必要なメモリ量と、使用可能なメモリ量を超過した量が示されます。アラートが出た場合は、設定を再評価してください。アクセス制御のルールまたは侵入ポリシーの数または複雑さを軽減できる場合があります。
接続統計情報	メトリック	接続の統計情報と NAT 変換カウントをモニターします。
CPUコア使用率	メトリック	CPU コア使用率が設定可能なしきい値を超えたときにアラートを出します。このモジュールを使用すると、メトリックの収集を中断することなく、正常性アラートの受信を有効または無効にできます。
Critical Process Statistics	メトリック	クリティカルプロセスの状態（リソース消費量と再起動回数）をモニタリングします
データベース	Alert	• スキーマまたは設定データに関連するデータベース整合性の問題についてシステムをモニターします。データベース整合性の問題に関するアラートを受信した場合は、Cisco TAC にお問い合わせください。データベースの整合性の問題があると、アップグレードが妨げられる可能性があります。 • 取り消しログ ファイルのサイズを監視し、サイズがしきい値制限を超えている場合はアラートを生成します。取り消しログには、変更前のデータの以前の状態が記録され、変更を元に戻すことが可能です。 • 取り消しログファイルのサイズが 800 MB を超え、1 GB 未満の場合、警告アラートが生成されます。 • クリティカルアラートは、取り消しログファイルのサイズが 1 GB を超えると生成されます。 デフォルトのしきい値を変更するには、Cisco TAC に連絡してください。
データプレーン CPU 使用率	メトリック	データ プレーンの CPU 使用率が設定可能なしきい値を超えたときにアラートを出します。このモジュールを使用すると、メトリックの収集を中断することなく、正常性アラートの受信を有効または無効にできます。
データプレーンメモリ使用率	メトリック	データ プレーンのメモリ使用量が設定可能なしきい値を超えたときにアラートを発行します。このモジュールを使用すると、メトリックの収集を中断することなく、正常性アラートの受信を有効または無効にできます。
Deployed Configuration Statistics	メトリック	展開された設定に関する統計情報（ACE の数や IPS ルールの数など）をモニターします。

モジュール	タイプ	説明
ディスク ステータス	Alert	ハードディスクまたは RAID コントローラに問題がある場合にアラートを出します。このモジュールがアラートを示した場合は、Cisco TAC にお問い合わせください。これにより、アップグレードが防止されます。
ディスク使用量	メトリック	このモジュールは、アプライアンスのハード ドライブ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しきい値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。ディスク使用率アラートのトラブルシューティング シナリオについては、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を参照してください。 デバイス設定履歴ファイルのサイズが許容制限サイズを超えると、[ディスク使用量（Disk Usage）] モジュールから正常性アラートが送信されます。ディスク使用率アラートのトラブルシューティング シナリオについては、「デバイス設定履歴ファイルの正常性モニタリングアラートのディスク使用量」 を参照してください。この正常性アラートは、Secure Firewall Management Center のバージョン 7.2.0 ～ 7.2.5、7.3.x、および 7.4.0 ではサポートされていません。 ディスク使用率ヘルス ステータス モジュールは、アプライアンス上の `/` パーティションと `/volume` パーティションのディスク使用率を監視して、ドレイン頻度を追跡するために使用します。ディスク使用率モジュールは `/boot` パーティションを監視対象パーティションとして列挙しますが、そのパーティションのサイズが固定のため、このモジュールはブート パーティションに基づいてアラートを出すことはしません。 **[ディスク領域のクリア（Clear disk space）]** オプションを使用して、Threat Defense デバイスから一時ファイルを削除してディスク領域を解放します。詳細については、「ディスク容量のクリア」を参照してください。
ファイルシステムの整合性チェック	Alert	このモジュールは、システムで CC モードまたは UCAPL モードが有効になっている場合、またはシステムが DEV キーで署名されたイメージを実行している場合に、ファイルシステムの整合性チェックを実行します。
Firewall Threat Defense HA	Alert	Threat Defense 高可用性ペアがスプリット ブレインされている場合にアラートを出します。

モジュール	タイプ	説明
Firewall Threat Defense のプラットフォームの障害	Alert	Cisco Secure Firewall 1000/3100/4200 プラットフォームの障害を監視し、障害に関する正常性アラートを生成します。 プラットフォーム障害は、Firewall Threat Defense インスタンスの障害や、発生したしきい値のアラームを表します。プラットフォーム障害のライフサイクルの間に、障害の状態またはシビラティ（重大度）が変化する場合があります。各障害には、障害の発生時に影響を受けたオブジェクトの動作状態に関する情報が含まれます。障害の状態が移行して解決すると、そのオブジェクトは機能状態に移行します。詳細については、『*Cisco Firepower 1000/2100 FXOS Faults and Error Messages Guide*』を参照してください。
フローオフロード統計情報	メトリック	ハードウェア フロー オフロードをモニターします。
FXOSの正常性	Alert	FXOS https サービスがデバイスで実行されていない場合にアラートを出します。これにより、アップグレードが防止されます。
ハードウェア アラーム	Alert	このモジュールは、物理管理対象デバイス上のハードウェアを交換する必要があるかどうかを確認し、ハードウェア ステータスに基づいてアラートを出します。ハードウェア関連デーモンのステータスについても報告します。
インライン リンク不一致アラーム	Alert	インライン ペア インターフェイスが異なる速度をネゴシエートした場合にアラートを出します。

モジュール	タイプ	説明
インターフェイス統計情報	Alert	デバイスが現在トラフィックを収集しているかどうかを確認して、物理インターフェイスおよび集約インターフェイスのトラフィック ステータスに基づいてアラートを出します。物理インターフェイスの情報には、インターフェイス名、リンク ステート、および帯域幅が含まれます。集約インターフェイスの情報には、インターフェイス名、アクティブ リンクの数、および総集約帯域幅が含まれます。 （注） このモジュールは、高可用性スタンバイデバイスのトラフィックフローも監視します。スタンバイデバイスがトラフィックを受信していないことがわかっていても、Firewall Management Center はインターフェイスがトラフィックを受信していないことを警告します。ポートチャネルの一部のサブインターフェイスでトラフィックが受信されない場合も、同じアラートの原則が適用されます。 このモジュールは、Linaからの値に従ってトラフィックレートを表示します。**show interface** CLI コマンドを使用してデバイスのインターフェイス統計を確認する場合、CLI コマンドの結果の入出力レートは、この**インターフェイス** ウィジェットに表示されるトラフィック レートと異なる場合があります。Lina と Firewall Management Center インターフェイス統計のサンプリング間隔は異なります。サンプリング間隔の違いにより、Firewall Management Center GUI のスループット値が CLI の結果に表示されるスループット値と異なる場合があります。 **[インターフェイス トラフィックレート（Interface Traffic Rate）]** ウィジェット（**[概要（Overview）]** > **[ダッシュ ボード（Dashboards）** > **] ダッシュボード** ページ）のトラフィックレートは、Snort からの入力レートと出力レートが表示されるため、異なる場合があることに注意してください。
侵入およびファイルイベント レート	Alert	1秒あたりの侵入イベント数が設定可能なしきい値を超えた場合にアラートを生成します。 警告しきい値は平均侵入イベントレートの 1.5 倍、クリティカルしきい値は 2.5 倍にすることをお勧めします。たとえば、1 秒あたり 20 イベントの平均イベントレートの場合、警告値を 30、クリティカル値を 50 にすることが推奨されます。クリティカル制限は 1000 よりも小さく、警告制限よりも大きくする必要があります。 デバイスのイベントレートは、[システム（System）]（⚙） > **[モニタリング（Monitoring）]** > **[統計（Statistics）]**で利用できます。レートが 0 の場合は、Snort プロセスがダウンしているか、デバイスがイベントを送信していない可能性があります。
リンク ステート伝達	Alert	ISA 3000 の場合、インライン セット内のインターフェイスで障害が発生した場合にアラートを出します。

モジュール	タイプ	説明
メモリ使用率	Alert	メモリ使用率が設定可能なしきい値を超えたときにアラートを発行します。 メモリが 4 GB を超えるアプライアンスの場合、プリセットされたアラートしきい値は、システム問題を引き起こす可能性のあるメモリ空き容量の割合を求める式に基づいています。4 GB を超えるのアプライアンスでは、警告しきい値と重大しきい値の時間間隔が非常に狭いため、[警告しきい値%（Warning Threshold %）] の値を手動で 50 に設定することを推奨します。これにより、時間内にアプライアンスのメモリ アラートを受け取って問題を解決できる可能性がさらに高まります。しきい値の計算方法の詳細については、ヘルスモニターアラートのメモリ使用率しきい値を参照してください。 複雑なアクセス コントロール ポリシーやルールは、重要なリソースを消費し、パフォーマンスに悪影響を与える可能性があります。
ネットワークカードのリセット	Alert	ハードウェア障害によりネットワークカードが再起動したときにアラートを出します。
NTP 統計情報	メトリック	NTP 同期ステータスをモニターします。デフォルトでは、ディセーブルです。
アウトオブバンド設定の変更	Alert	このモジュールは、**configure network management-data-interface** コマンドを直接使用して Firewall Management Center で行われた 設定の変更をモニターします。このモジュールは、既存の Firewall Management Center 設定とアウト オブ バンド設定の変更との間に競合がある場合にアラートを出します。
パスモニタリング	メトリック	インターフェイスでパスモニタリングが有効になっている場合、インターフェイスのデータ パス メトリックをモニターします。
Process Status	Alert	アプライアンス上のプロセスがプロセス マネージャの外部で停止または終了した場合にアラートを出します。 プロセスが故意にプロセス マネージャの外部で停止された場合は、モジュールが再開してプロセスが再起動するまで、モジュール ステータスが Warning に変更され、ヘルス イベント メッセージが停止されたプロセスを示します。プロセスがプロセス マネージャの外部で異常終了またはクラッシュした場合は、モジュールが再開してプロセスが再起動するまで、モジュール ステータスが Critical に変更され、ヘルス イベント メッセージが終了したプロセスを示します。
ルーティング統計情報	メトリック	ルーティングテーブルの現在の状態をモニターします
SD-WANモニタリング	メトリック	SD-WAN インターフェイスのアプリケーション パフォーマンス メトリックをモニターします。
Snort3統計情報	メトリック	イベント、フロー、およびパケットの Snort 3 統計情報を収集します。

モジュール	タイプ	説明
Snort の CPU 使用率	メトリック	このモジュールは、デバイス上の Snort プロセスの平均 CPU 使用率が過負荷になっていないことを確認し、CPU 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場合にアラートを出します。[Warning Threshold %] のデフォルト値は 80 です。[Critical Threshold %] のデフォルト値は 90 です。このモジュールを使用すると、メトリックの収集を中断することなく、正常性アラートの受信を有効または無効にできます。
Snortアイデンティティメモリ使用率	Alert	Snort アイデンティティ処理の警告しきい値の設定を可能にするとともに、メモリ使用率がモジュールに設定されたレベルを超えるとアラートを生成します。[クリティカルしきい値（%）（Critical Threshold %）] のデフォルト値は 80 です。 このヘルスモジュールは、Snort のユーザーアイデンティティ情報に使用される合計領域を具体的に追跡します。現在のメモリ使用量の詳細、ユーザー/IP バインディングの合計数、およびユーザーグループマッピングの詳細が表示されます。Snort はこれらの詳細をファイルに記録します。メモリ使用率ファイルが使用できない場合は、このモジュールのヘルスアラートに「Waiting for data」と表示されます。これは、新しいインストールまたはメジャーアップデート、Snort 2 から Snort 3 の切り替え、またはその逆への切り替え、あるいはメジャーポリシーの展開によって、Snort の再起動中に発生する可能性があります。ヘルスモニタリングサイクルに応じ、かつ、ファイルが使用可能になると、警告が消え、ヘルスモニターにこのモジュールの詳細が表示され、そのステータスはグリーンになります。
Snortメモリ使用率	メトリック	このモジュールは、割り当て済みメモリの Snort プロセスが占める割合を確認し、メモリ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場合にアラートを出します。[Warning Threshold %] のデフォルト値は 80 です。[Critical Threshold %] のデフォルト値は 90 です。このモジュールを使用すると、メトリックの収集を中断することなく、正常性アラートの受信を有効または無効にできます。
Snort 再設定検出	メトリック	デバイスの再設定が失敗した場合、アラートを出します。このモジュールは、Snort 2 と Snort 3 の両方のインスタンスの再設定失敗を検出します。
Snort Statistics	メトリック	イベント、フロー、およびパケットの Snort 統計情報をモニターします。
SSE 接続ステータス	メトリック	このモジュールは、デバイスが Security Services Exchange クラウドに最初は正常に接続でき、その後接続できなくなった場合にアラートを出します。デフォルトでは、ディセーブルです。

モジュール	タイプ	説明
システム CPU 使用率	メトリック	このモジュールは、デバイス上のすべてのシステムプロセスの平均 CPU 使用率が過負荷になっていないことを確認し、CPU 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場合にアラートを出します。[Warning Threshold %] のデフォルト値は 80 です。[Critical Threshold %] のデフォルト値は 90 です。このモジュールを使用すると、メトリックの収集を中断することなく、正常性アラートの受信を有効または無効にできます。
Talos接続ステータス	Alert	URL のレピュテーションと分類のために URL フィルタリングデータベースを定期的に更新するために必要な、Talos クラウドサービスとの 接続をモニターします。

モジュール	タイプ	説明
デバイスでの脅威データの更新	Alert	

モジュール	タイプ	説明
		デバイスが脅威の検出に使用する特定のインテリジェンスデータと設定は、Firewall Management Center 上で 30 分ごとにクラウドから更新されます。 このモジュールは、指定した期間内にデバイスでこの情報が更新されない場合にアラートを生成します。 モニターされる更新には次の点が含まれます。 • ローカル URL カテゴリおよびレピュテーション データ • セキュリティ インテリジェンス URL リストおよびフィード（Threat Intelligence Director からのグローバルブロックリストとブロックしないリストおよび URLを含む） • セキュリティ インテリジェンス ネットワーク リストおよびフィード（IP アドレス）（Threat Intelligence Director からのグローバルブロックリストとブロックしないリストおよび IP アドレスを含む） • セキュリティ インテリジェンス DNS リストおよびフィード（Threat Intelligence Director からのグローバルブロックリストとブロックしないリストおよびドメインを含む） • （ClamAV からの）ローカル マルウェア分析の署名 • Threat Intelligence Director からの SHA リスト（[オブジェクト（Objects）] >[オブジェクト管理（Object Management）]>[セキュリティ インテリジェンス（Security Intelligence）] > [ネットワーク リストおよびフィード（Network Lists and Feeds）] ページにリストされている） • [統合（Integration）] > [AMP] > [動的分析接続（Dynamic Analysis Connections）] ページで設定された動的分析の設定 • キャッシュされた URL の期限切れに関連する [脅威設定（Threat Configuration）] の設定（**[統合（Integration）]** > **[その他の統合（Other Integrations）]** > **[クラウドサービス（Cloud Services）]** ページの [キャッシュされたURLの期限切れ（Cached URLs Expire）] の設定を含む）（このモジュールでは、URL キャッシュの更新はモニターされません。） • イベントを送信するためのシスコ クラウドとの通信の問題。**[統合（Integration）]** > **[その他の統合（Other Integrations）]** > [クラウドサービス（Cloud Services）] ページの [シスコクラウド（Cisco Cloud）] ボックスを確認します。 （注） システムに Threat Intelligence Director が設定されており、フィードがある場合にのみ、TID の更新が含まれます。 デフォルトでは、このモジュールは 1 時間後に警告を送信し、24 時間後に重大なアラートを送信します。

モジュール	タイプ	説明
		Firewall Management Center またはいずれかのデバイスで障害が発生していることをこのモジュールが示している場合、Firewall Management Center がデバイスに到達できることを確認します。
VPN 統計情報	メトリック	Firewall Threat Defense デバイス間のサイト間およびリモート アクセス VPN トンネルをモニターします。
XTLS カウンタ	メトリック	XTLS/SSL フロー、メモリ、およびキャッシュの有効性をモニターしますデフォルトでは、ディセーブルです。

表 *2 : Management Center* の正常性モジュール

モジュール	タイプ	説明
Secure Endpoint のステータス	アラート	このモジュールは、Firewall Management Center が初期接続の成功後に AMP クラウドまたは Cisco AMP Private Cloud に接続できない場合、またはプライベートクラウドがパブリック AMP クラウドに接続できない場合にアラートを出します。また、Secure Endpoint 管理コンソールを使用して AMP クラウド接続の登録が解除された場合にもアラートを出します。
AMP for Firepower のステータス	Alert	以下の場合にアラートを出します： • Firewall Management Center が AMP クラウド（パブリックまたはプライベート）、Secure Malware Analytics クラウドまたはアプライアンスに接続できないか、または AMP プライベートクラウドがパブリック AMP クラウドに接続できない。 • 接続に使用する暗号化キーが無効である。 • デバイスが Secure Malware Analytics クラウドまたは Secure Malware Analytics アプライアンスに接続して動的分析用のファイルを送信できない。 • ファイル ポリシー設定に基づいてネットワーク トラフィックで過剰な数のファイルが検出された。 Firewall Management Center のインターネット接続が切断された場合、ヘルスアラートの生成に最大 30 分かかることがあります。
アプライアンス ハートビート	Alert	このモジュールは、アプライアンス ハートビートがアプライアンスから届いているかどうかを確認し、アプライアンスのハートビート ステータスに基づいてアラートを出します。
証明書のモニタリング	Alert	サービス認証証明書の有効期限に近づいているか、または期限切れになったときに、設定可能なしきい値（日数単位）に基づいてアラートを発行します。サービスの中断を避けるには、期限切れになる前に証明書を更新してください。

モジュール	タイプ	説明
CPUコア使用率	メトリック	このモジュールは、すべてのコアの CPU 使用率が過負荷になっていないことを確認し、CPU 使用率がモジュールに設定されたしきい値を超えた場合にアラートを出します。[Warning Threshold %] のデフォルト値は 80 です。[Critical Threshold %] のデフォルト値は 90 です。このモジュールはデフォルトでは有効になっています。 メトリックの収集を中断することなく、このモジュールの正常性アラートの受信を有効または無効にできます。
Critical Process Statistics	メトリック	クリティカルプロセスの状態（リソース消費量と再起動回数）をモニタリングします
CSDAC ダイナミック属性コネクタ		
データベース	Alert	設定データベースのサイズが大きすぎる場合にアラートを発行します。 また、データベーススキーマまたは設定データ（*EO*と呼ばれることもあります）の整合性の問題がないかモニターします。このモジュールがアラートを示した場合は、Cisco TAC にお問い合わせください。これにより、アップグレードが防止されます。
ディスカバリホスト制限	Alert	このモジュールは、Firewall Management Center がモニターできるホスト数が制限に近づいているかどうかを確認し、モジュールに設定された警告レベルに基づいてアラートを出します。詳細については、ホスト制限（Host Limit）を参照してください。
ディスク ステータス	Alert	このモジュールは、ハードディスクと、アプライアンス上のマルウェアストレージパック（設置されている場合）のパフォーマンスを調査します。 このモジュールは、ハードディスクと RAID コントローラ（設置されている場合）で障害が発生する恐れがある場合、または、マルウェア ストレージ パックではない追加のハードドライブが設置されている場合に、警告（黄色）ヘルス アラートを生成します。また、設置されているマルウェア ストレージ パックを検出できなかった場合はアラート（赤色）ヘルス アラートを生成します。

モジュール	タイプ	説明
ディスク使用量	メトリック	このモジュールは、アプライアン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しきい値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。ディスク使用率アラートのトラブルシューティングシナリオについては、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を参照してください。 デバイス設定履歴ファイルのサイズが許容制限サイズを超えると、[ディスク使用量（Disk Usage）] モジュールから正常性アラートが送信されます。ディスク使用率アラートのトラブルシューティング シナリオについては、「デバイス設定履歴ファイルの正常性モニタリングアラートのディスク使用量」 を参照してください。この正常性アラートは、Secure Firewall Management Center のバージョン 7.2.0 ～ 7.2.5、7.3.x、および 7.4.0 ではサポートされていません。 ディスク使用率ヘルス ステータス モジュールは、アプライアンス上の / パーティションと /volume パーティションのディスク使用率を監視して、ドレイン頻度を追跡するために使用します。ディスク使用率モジュールは /boot パーティションを監視対象パーティションとして列挙しますが、そのパーティションのサイズが固定のため、このモジュールはブート パーティションに基づいてアラートを出すことはしません。 **[ディスク領域のクリア（Clear disk space）]** オプションを使用して、Firewall Management Center から一時ファイルを削除してディスク領域を解放します。詳細については、「ディスク容量のクリア」を参照してください。
eStreamステータス	Alert	Firewall Management Center の Event Streamer を使用するサードパーティ製クライアント アプリケーションへの接続をモニタリングします。
イベント バックログ ステータス	Alert	デバイスから Firewall Management Center に送信されるのを待機しているイベント データのバックログのサイズが、30 分を超えて増大し続けた場合にアラートを発します。 バックログを減らすには、帯域幅を評価し、ログに記録するイベント数を減らすことを検討してください。
Event Monitor	メトリック	このモジュールは、Firewall Management Center への全体の着信イベントレートをモニターします。
ファイルシステムの整合性チェック	Alert	このモジュールは、システムで CC モードまたは UCAPL モードが有効になっている場合、またはシステムが DEV キーで署名されたイメージを実行している場合に、ファイルシステムの整合性チェックを実行します。このモジュールはデフォルトでは有効になっています。

モジュール	タイプ	説明
Firewall Management Center の HA ステータス	Alert	Firewall Management Center 高可用性のモニターHA ペアが同期されず、アクティブ ユニットとスタンバイ ユニット間で管理対象デバイスの数に不一致がある場合、このモジュールはアラートを生成します。
Firewall Threat Defense HA	Alert	Threat Defense 高可用性ペアがスプリット ブレインされている場合にアラートを出します。
ハードウェア統計情報	メトリック	Firewall Management Center ハードウェアをモニターします（ファン速度、温度、電源）。値が設定可能なしきい値を超えた場合にアラートを生成します。
ヘルス モニター プロセス	Alert	正常性プロセス自体をモニターし、指定した分数（設定可能）内に正常性イベントが発生していない場合にアラートを出します。
ISE 接続のモニター	Alert	このモジュールは、Cisco Identity Services Engine（ISE）と Firewall Management Center 間のサーバー接続のステータスをモニターします。ISE は、追加のユーザー データ、デバイス タイプ データ、デバイス ロケーション データ、SGT（セキュリティ グループ タグ）、および SXP（Security Exchange Protocol）サービスを提供します。
ローカル マルウェア分析	Alert	このモジュールはローカル マルウェア分析の ClamAV 更新をモニターします。

モジュール	タイプ	説明
メモリ使用率	Alert	このモジュールは、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、使用率がモジュールに設定されたレベルを超えるとアラートを出します。 メモリ使用率を計算する場合、Firewall Management Center メモリ使用率正常性モジュールは、RAM、スワップメモリ、キャッシュメモリの使用率をモニタリングし、計算に含めます。 メモリが 4 GB を超えるアプライアンスの場合、プリセットされたアラートしきい値は、システム問題を引き起こす可能性のあるメモリ空き容量の割合を求める式に基づいています。4 GB を超えるのアプライアンスでは、警告しきい値と重大しきい値の時間間隔が非常に狭いため、[警告しきい値%（Warning Threshold %）] の値を手動で 50 に設定することを推奨します。これにより、時間内にアプライアンスのメモリ アラートを受け取って問題を解決できる可能性がさらに高まります。しきい値の計算方法の詳細については、ヘルスモニターアラートのメモリ使用率しきい値を参照してください。 バージョン 6.6.0 以降では、バージョン 6.6.0 以降への Firewall Management Center Virtual のアップグレードに必要な最小 RAM 容量は 28 GB であり、Firewall Management Center Virtual の展開に推奨される RAM 容量は 32 GB です。デフォルト設定（ほとんどの Firewall Management Center Virtual インスタンスでは 32 GB、Firewall Management Center Virtual 300 では 64 GB の RAM）の値は小さくしないことをお勧めします。 **注目** Firewall Management Center Virtual 展開に割り当てられた RAM が不十分である場合、ヘルスモニターによってクリティカルアラートが生成されます。 Firewall 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 Firewall Management Center を再起動する可能性があります。 複雑なアクセス コントロール ポリシーやルールは、重要なリソースを消費し、パフォーマンスに悪影響を与える可能性があります。
MariaDB 統計	メトリック	このモジュールは、MariaDB データベースのサイズ、アクティブな接続数、メモリ使用量など、MySQL データベースのステータスをモニターします。
MonetDB統計	メトリック	MonetDB はファイアウォール イベント、および接続サマリーなどのイベント関連データのデータベースです。この正常性モジュールは、サイズ、アクティブな接続数、メモリ使用量など、MonetDB データベースのステータスをモニターします。さらに、処理されているデータ要求の数をモニターし、低速実行の要求を特定することもできます。

モジュール	タイプ	説明
パッシブIDエージェントモニター	Alert	Firewall Management Center と、それがインストールされているマシン間の接続エラーを表示します。 パッシブ ID エージェント は定期的に更新情報を Firewall Management Center に送信します。この正常性アラートは、Firewall Management Center が パッシブ ID エージェント からエラーを受信した場合、または Firewall Management Center が 5 分以上更新または応答を受信していない場合に表示されます。 2 つの間の接続を確認し、パッシブ ID エージェント ソフトウェアを再起動して、数分後に正常性アラートを再度確認してください。 問題が解決しない場合は、**[統合（Integration）] > [その他の統合（Other Integrations）] > [アイデンティティソース（Identity Sources）]**で設定を確認してください。
Process Status	Alert	アプライアンス上のプロセスがプロセス マネージャの外部で停止または終了した場合にアラートを出します。 プロセスが故意にプロセス マネージャの外部で停止された場合は、モジュールが再開してプロセスが再起動するまで、モジュール ステータスが Warning に変更され、ヘルス イベント メッセージが停止されたプロセスを示します。プロセスがプロセス マネージャの外部で異常終了またはクラッシュした場合は、モジュールが再開してプロセスが再起動するまで、モジュール ステータスが Critical に変更され、ヘルス イベント メッセージが終了したプロセスを示します。
RabbitMQ ステータス	メトリック	RabbitMQ 統計をモニタリングし、収集します

モジュール	タイプ	説明
Realm	Alert	レルムまたはユーザーの不一致の次のような警告しきい値を設定できます。 • ユーザーの不一致：ユーザーは、ダウンロードされることなく Secure Firewall Management Center に報告されます。 ユーザーの不一致の一般的な理由は、ユーザーが Secure Firewall Management Center へのダウンロードから除外されたグループに属していることです。Review the information discussed in Cisco Secure Firewall Management Center デバイス構成ガイド. • レルムの不一致：ユーザーが、Firewall Management Center に認識されていないレルムに対応するドメインにログインした場合に不一致が起きます。 詳細については、Cisco Secure Firewall Management Center デバイス構成ガイドを参照してください。 このモジュールは、レルムごとにサポートされているダウンロードユーザーの最大数よりも多くのユーザーをダウンロードしようとすると、正常性アラートも表示します。単一のレルムのダウンロードユーザーの最大数は、管理センターのモデルによって異なります。 詳細については、Cisco Secure Firewall Management Center デバイス構成ガイドのユーザー制限を参照してください。
RRD サーバー プロセス	Alert	時系列データを格納するラウンドロビン データ（RRD）サーバーが前回の更新以降に再起動した場合にアラートを出します。連続した再起動に対する追加の警告とクリティカルのしきい値を設定できます。
セキュリティ インテリジェンス（Security Intelligence）	Alert	セキュリティ インテリジェンスが使用中であり、Firewall Management Center がフィードを更新できないか、フィードデータが破損している、またはフィードデータに認識可能な IP アドレスが含まれていない場合にアラートを発します。 Threat Data Updates on Devices モジュールも参照してください。
スマート ライセンス モニター	Alert	スマート ライセンスのステータスをモニタリングし、以下の場合にアラートを送信します。 • Smart Licensing Agent（スマートエージェント）と Smart Software Manager (SSM) の間の通信にエラーがある。 • 製品インスタンス登録トークンの有効期限が切れている。 • スマート ライセンスの使用状況がコンプライアンスに違反している。 • スマート ライセンスの権限モードまたは評価モードの有効期限が切れている。

モジュール	タイプ	説明
Talos接続ステータス	Alert	URL フィルタリングおよびイベントエンリッチメント データのダウンロードに必要な Talos との 接続をモニターします。

モジュール	タイプ	説明
デバイスでの脅威データの更新	Alert	

モジュール	タイプ	説明
		デバイスが脅威の検出に使用する特定のインテリジェンスデータと設定は、Firewall Management Center 上で 30 分ごとにクラウドから更新されます。 このモジュールは、指定した期間内にデバイスでこの情報が更新されない場合にアラートを生成します。 モニターされる更新には次の点が含まれます。 • ローカル URL カテゴリおよびレピュテーション データ。 • セキュリティ インテリジェンス URL リストおよびフィード（Threat Intelligence Director からのグローバルブロックリストと ブロックしないリストおよび URLを含む）。 • セキュリティ インテリジェンス ネットワーク リストおよびフィード（IP アドレス）（Threat Intelligence Director からのグローバルブロックリストと ブロックしない リストおよび IP アドレスを含む）。 • セキュリティ インテリジェンス DNS リストおよびフィード（Threat Intelligence Director からのグローバル ブロック リストと ブロックしないリストおよびドメインを含む）。 • （ClamAV からの）ローカル マルウェア分析の署名。 • Threat Intelligence Director からの SHA リスト（**[オブジェクト（Objects）]> [オブジェクト管理（Object Management）] > [セキュリティ インテリジェンス（Security Intelligence）] > [ネットワーク リストおよびフィード（Network Lists and Feeds）]** ページにリストされている）。 • **[統合（Integration）] > [AMP] > [動的分析接続（Dynamic Analysis Connections）]** ページで設定された動的分析の設定。 • キャッシュされた URL の期限切れに関連する [脅威設定（Threat Configuration）] の設定（**[統合（Integration）] > [その他の統合（Other Integrations）] > [クラウドサービス（Cloud Services）]** ページの [キャッシュされたURLの期限切れ（Cached URLs Expire）] の設定を含む）（このモジュールでは、URL キャッシュの更新はモニターされません。） • イベントを送信するためのシスコ クラウドとの通信の問題。**[統合（Integration）] > [その他の統合（Other Integrations）]** > [クラウドサービス（Cloud Services）] ページの [シスコクラウド（Cisco Cloud）] ボックスを確認します。 （注） システムに Threat Intelligence Director が設定されており、フィードがある場合にのみ、TID の更新が含まれます。 デフォルトでは、このモジュールは 1 時間後に警告を送信し、24 時間後に重大なアラートを送信します。

モジュール	タイプ	説明
		Firewall Management Center またはいずれかのデバイスで障害が発生していることをこのモジュールが示している場合、Firewall Management Center がデバイスに到達できることを確認します。
時系列データ（RRD）モニター	Alert	このモジュールは、時系列データ（相関イベント カウントなど）が保存されるディレクトリ内の破損ファイルの存在を追跡して、ファイルが破損としてフラグが付けられ、削除された段階でアラートを出します。
タイムサーバーステータス	Alert	このモジュールは NTP サーバーの設定をモニターし、NTP サーバーが使用できない場合、またはNTPサーバーの設定が無効な場合にアラートを出します。 このモジュールから重大なアラートを受信した場合は、[システム（System）]（⚙） > **[設定（Configuration）]** > **[時刻の同期（Time Synchronization ）]** を選択し、アラートで指定されている NTP サーバーの設定を確認します。
時刻同期ステータス	Alert	このモジュールは、NTP を使用して時刻を取得するデバイス クロックと NTP サーバー上のクロックの同期を追跡して、クロックの差が 10 秒を超えた場合にアラートを出します。
未解決グループモニター	Alert	ポリシーで使用されるグループである Foreign Security Principal（FSP）を監視します。セキュリティ プリンシパルは、アクセス コントロール ポリシーでセキュリティを適用できる認証済みユーザー グループなどの Active Directory オブジェクトです。 このモジュールは、存在しているもののポリシーで使用されていない未解決グループに関する警告アラートと、ポリシーで使用されている未解決グループの重大なアラートを生成します。
URL フィルタリング モニター	Alert	URL フィルタリングデータのダウンロードと URL フィルタリングルックアップの実行に必要な Cisco Cloud との の接続をモニターします。
Web サーバー接続統計	メトリック	単一の IP アドレスが、Management Center の Web サーバーへの同時 HTTP または HTTPS 接続の設定可能な制限を超えると警告します。単一の IP アドレスから管理センターに接続するために最大数のブラウザ タブが開かれると、警告が表示されます。これにより、最適なパフォーマンスが確保されます。
ゼロ タッチ プロビジョニング	Alert	シリアル番号を使用したデバイスの登録中に障害が発生した場合にアラートを出します。また、高可用性の ゼロタッチプロビジョニング 対応 Firewall Management Center に関連するエラーも表示されます。

ヘルス モニタリングの設定

手順

ステップ 1 ヘルス モジュール （3 ページ）で説明されているように、モニターするヘルス モジュールを決定します。

Firepower システムで使用しているアプライアンスの種類ごとに固有のポリシーをセットアップして、そのアプライアンスに適切なテストだけを有効にすることができます。

ヒント
モニタリング動作をカスタマイズすることなくすぐにヘルスモニタリングを有効にするには、そのために用意されたデフォルト ポリシーを適用できます。

ステップ 2 正常性ポリシーの作成 （26 ページ）で説明されているように、ヘルス ステータスを追跡するアプライアンスごとに正常性ポリシーを適用します。

ステップ 3 （オプション）ヘルス モニター アラートの作成 （42 ページ）で説明されているように、ヘルス モニタ アラートを設定します。

ヘルス ステータス レベルが特定のヘルス モジュールの特定の重大度レベルに達した段階でトリガーされる電子メール、Syslog、または SNMP アラートをセットアップできます。

正常性ポリシー

正常性ポリシーには、複数のモジュールに対して設定可能な正常性テスト基準が含まれます。アプライアンスごとにどのヘルス モジュールを実行するかを制御したり、モジュールごとに実行するテストで使用される特定の制限を設定したりできます。

正常性ポリシーを設定するときに、そのポリシーに対して各ヘルスモジュールを有効にするかどうかを決定します。また、有効にした各モジュールが、プロセスの正常性を評価するたびに報告するヘルス ステータスを制御するための基準を選択することもできます。

正常性モジュール内の個々の属性に関して正常性アラートを有効または無効にできます。属性レベルで正常性アラートの設定を調整することにより、正常性アラートの数を減らし、データ収集を中断することなく、最も重要な正常性アラートに効率的に焦点を合わせることができます。引き続き、[正常性モニター（Health Monitor）] ダッシュボードから属性をモニターできます。正常性ポリシーで正常性モジュールを有効にすると、その正常性モジュールに含まれるすべての属性の正常性アラート設定がデフォルトで有効になります。

システム内のすべてのアプライアンスに適用可能な 1 つの正常性ポリシーを作成することも、適用を計画している特定のアプライアンス用に正常性ポリシーをカスタマイズすることも、付属のデフォルト正常性ポリシーを使用することもできます。

（注） アプライアンスを登録すると、Firewall Management Center によってデフォルトの正常性ポリシーが自動的に割り当てられます。正常性ポリシーとアプライアンスの関連付けを解除するには、まず、別の正常性ポリシーをアプライアンスに関連付ける必要があります。アプライアンスには、少なくとも 1 つの正常性ポリシーが割り当てられている必要があります。

デフォルトの正常性ポリシー

Firewall Management Center セットアッププロセスは、使用可能な正常性モジュールのほとんど（すべてではない）が有効になっている初期正常性ポリシーを作成して適用します。

この初期の正常性ポリシーは、デフォルトの正常性ポリシーに基づいています。デフォルトの正常性ポリシーは、表示も編集もできませんが、カスタム正常性ポリシーを作成するときにコピーできます。

カスタムの正常性ポリシーを作成して、デフォルトの正常性ポリシーとして設定することができます。デバイスを Firewall Management Center に追加すると、Firewall Management Center は管理対象デバイスにデフォルトの正常性ポリシーを適用します。デフォルトとして設定した正常性ポリシーは削除できないことに注意してください。デフォルトの正常性ポリシーを設定する詳細な手順については、デフォルトの正常性ポリシーの設定 （30 ページ）を参照してください。

アップグレードとデフォルトの正常性ポリシー

Firewall Management Center をアップグレードすると、新しい正常性モジュールがすべての正常性ポリシーに追加されます。これには、初期の正常性ポリシー、デフォルトの正常性ポリシー、およびその他のカスタム正常性ポリシーが含まれます。通常、新しい正常性モジュールは有効な状態で追加されます。

（注） 新しい正常性モジュールでモニタリングとアラートを開始するには、アップグレード後に正常性ポリシーを再適用します。

正常性ポリシーの作成

アプライアンスで使用する正常性ポリシーをカスタマイズすることによって、新しいポリシーを作成できます。ポリシー内の設定は、最初に、新しいポリシーの基準として選択した正常性ポリシー内の設定を使用して生成されます。ポリシーを編集して、ポリシー内のモジュールの有効化または無効化などの設定を指定したり、必要に応じて各モジュールのアラート基準を変更したり、実行時間間隔を指定したりできます。

手順

ステップ 1 [システム（System）]（⚙）>**[正常性（Health）]**>**[ポリシー（Policy）]**を選択します。

ステップ 2 [ポリシーの作成（Create Policy）] をクリックします。

ステップ 3 ポリシーの名前を入力します。

次の名前はデフォルトポリシー用に予約されており、これらの名前を使用して正常性ポリシーを作成することはできないことに注意してください。

- デフォルトのデバイス ポリシー
- デフォルトの正常性ポリシー

ステップ 4 [ベースポリシー（Base Policy）] ドロップダウンリストから、新しいポリシーの基準として使用する既存のポリシーを選択します。

ステップ 5 ポリシーの説明を入力します。

ステップ 6 **[保存（Save）]** を選択します。

次のタスク

- 正常性ポリシーの適用 （27ページ）で説明されているように、デバイスにヘルスポリシーを適用します。
- 正常性ポリシーの編集 （28 ページ）で説明されているように、ポリシーを編集して、モジュールレベルのポリシー設定を指定します。

正常性ポリシーの適用

正常性ポリシーをアプライアンスに適用すると、ポリシー内で有効にしたすべてのモジュールのヘルステストが、アプライアンス上のプロセスとハードウェアの正常性を自動的に監視します。その後、ヘルステストは、ポリシー内で設定された時間間隔で実行を続け、アプライアンスのヘルス データを収集し、そのデータをFirewall Management Centerに転送します。

正常性ポリシーでモジュールを有効にしてから、ヘルステストが必要ないアプライアンスにポリシーを適用した場合、ヘルス モニタはそのヘルス モジュールのステータスを無効として報告します。

すべてのモジュールが無効になっているポリシーをアプライアンスに適用すると、適用されたすべての正常性ポリシーがアプライアンスから削除されるため、どの正常性ポリシーも適用されません。ただし、アプライアンスには少なくとも1つの正常性ポリシーが割り当てられている必要があります。

すでにポリシーが適用されているアプライアンスに別のポリシーを適用した場合は、新しく適用されたテストに基づく新しいデータの表示が少し遅れる可能性があります。

手順

ステップ 1 [システム（System）]（⚙）>**[正常性（Health）]**>**[ポリシー（Policy）]** を選択します。

ステップ 2 適用するポリシーの横にある [正常性ポリシーの展開（Deploy health policy）]（📥） をクリックします。

ステップ 3 正常性ポリシーを適用するアプライアンスを選択します。

（注）
アプライアンスには、少なくとも 1 つの正常性ポリシーが割り当てられている必要があります。アプライアンスのヘルスモニタリングを停止するには、すべてのモジュールが無効になっている正常性ポリシーを作成し、それをアプライアンスに適用します。正常性ポリシーとアプライアンスの関連付けを解除するには、まず別の正常性ポリシーをアプライアンスに関連付ける必要があります。

ステップ 4 [適用（Apply）] をクリックして、選択したアプライアンスにポリシーを適用します。

次のタスク

- 必要に応じて、タスクのステータスをモニタします（タスクメッセージの表示を参照）。

  アプライアンスのモニタリングは、ポリシーが正常に適用されると開始されます。

正常性ポリシーの編集

変更する正常性ポリシーを編集できます。

手順

ステップ 1 [システム（System）]（⚙）>**[正常性（Health）]**>**[ポリシー（Policy）]**を選択します。

ステップ 2 変更するポリシーの横にある [編集（Edit）]（✎） をクリックします。

ステップ 3 ポリシー名とその説明を編集するには、ポリシー名に対して表示される [編集（Edit）]（✎）アイコンをクリックします。

ステップ 4 [ヘルスモジュール（Health Modules）] タブには、すべてのデバイスモジュールとその属性が表示されます。次のアクションを使用して、正常性モジュールを設定します。

- モジュールとその属性に対して表示されるトグルボタンをクリックします。オン（🔵）またはオフ（⚫）にして、それぞれヘルスステータスのテストを有効または無効にします。
- 正常性モジュールで一括有効化または無効化テストを実行するには、[すべて選択（Select All）] トグルボタンをクリックします。

- 正常性モジュールを有効にした後、利用可能な場合は、正常性モジュール内の個々の属性の横にあるチェックボックスを使用して、その属性の正常性アラートを有効または無効にします。属性の正常性アラートを無効にしても、その属性のメトリックの収集は停止しないことに注意してください。これらの属性は、[正常性モニター（Health Monitor）] ダッシュボードから引き続きモニターできます。

（注）
- モジュールと属性には、サポートしているアプライアンス（Firewall Threat Defense、Firewall Management Center、またはその両方）でフラグが付けられます。
- CPUおよびメモリモジュールの個々の属性を含めるか除外するかを選択することはできません。

モジュールについては、ヘルス モジュール （3 ページ）を参照してください。

ステップ 5 該当する場合は、[重大（Critical）] および [警告（Warning）] しきい値のパーセンテージを設定します。

ステップ 6 **[設定（Settings）]** タブで、フィールドに関連する値を入力します。

- **[ヘルスモジュールの実行間隔（Health Module Run Time Interval）]**：ヘルスモジュールを実行する頻度。最小の間隔は 5 分です。
- [メトリック収集間隔（Metric Collection Interval）]：デバイスとそのヘルスモジュールで時系列データを収集する頻度。デフォルトでは、デバイスモニターは、いくつかの事前定義されたヘルスモニターダッシュボードでこれらのメトリックを報告します。ダッシュボードの詳細については、ダッシュボードについてを参照してください。メトリックデータは分析のために収集されるため、アラートは関連付けられません。
- [OpenConfigストリーミングテレメトリ（OpenConfig Streaming Telemetry）]：ベンダー中立の OpenConfig モデルを使用する、Firewall Threat Defense デバイスから外部データ収集システムへのヘルス メトリクス テレメトリ ストリームを構成します。詳細については、OpenConfig ストリーミングテレメトリの設定を参照してください。

ステップ 7 ポリシーが割り当てられているデバイスを表示および変更するには、次の手順を実行します。

a) [ポリシーの割り当てと展開（Policy Assignments & Deploy）] をクリックします。
b) [使用可能なデバイス（Available Devices）] リストから、正常性ポリシーを割り当てるデバイスの横にある [+] アイコンをクリックします。
c) [適用（Apply）] をクリックします。

または、正常性ポリシーの適用 （27 ページ）の説明に従って、アプライアンスに正常性ポリシーを適用できます。

正常性ステータスを追跡するアプライアンスごとに正常性ポリシーを適用します。正常性ポリシーをアプライアンスに適用すると、ポリシー内で有効にしたすべてのモジュールが、アプライアンス上のプロセスとハードウェアの正常性をモニターし、そのデータを Firewall Management Center に転送します。

ステップ 8 [保存（Save）] をクリックします。

デフォルトの正常性ポリシーの設定

ユーザーが作成した正常性ポリシーをデフォルトの正常性ポリシーとして設定できます。デバイスを Firewall Management Center に追加すると、Firewall Management Center は管理対象デバイスにデフォルトの正常性ポリシーを適用します。

（注） 新しいデフォルトの正常性ポリシーを設定しても、すでに登録されているデバイスに割り当てられている正常性ポリシーには影響しません。

手順

ステップ 1 [システム（System）]（⚙） > **[正常性（Health）]** > **[ポリシー（Policy）]**を選択します。

ステップ 2 デフォルトとして設定する正常性ポリシーの横にある [その他のアクション（More Actions）]（⋮） アイコンをクリックし、[デフォルトとして設定（Set as Default）] をクリックします。

ステップ 3 [続行（Proceed）] をクリックします。

正常性ポリシーの削除

不要になった正常性ポリシーを削除できます。ただし、アプライアンスには少なくとも 1 つの正常性ポリシーが割り当てられている必要があります。アプライアンスに適用されているポリシーを削除した場合は、別のポリシーを適用するまでそのポリシー設定が有効のままになります。加えて、デバイスに適用されている正常性ポリシーを削除した場合、元となる関連アラート応答を無効にするまでは、そのデバイスに対して有効になっているヘルス モニタリング アラートがアクティブなままになります。

ヒント アプライアンスのヘルスモニタリングを停止するには、すべてのモジュールが無効になっている正常性ポリシーを作成し、それをアプライアンスに適用します。

手順

ステップ 1 [システム（System）]（⚙） > **[正常性（Health）]** > **[ポリシー（Policy）]**を選択します。

ステップ 2 削除するポリシーの横にある [削除（Delete）]（🗑） をクリックし、[正常性ポリシーの削除（Delete health policy）] をクリックして削除します。

デフォルトポリシーとして設定されている正常性ポリシーは削除できないことに注意してください。現在のデフォルトポリシーの削除を試みる前に、別の正常性ポリシーをデフォルトとして設定します。詳細については、「デフォルトの正常性ポリシーの設定 （30 ページ）」を参照してください。

OpenConfig を使用したベンダー中立のテレメトリストリーミングの送信

OpenConfig は、ネットワークを管理およびモニターするために単一の方法で複数のベンダーにネットワーク テレメトリ データをストリーミングすることを可能にする、ベンダーに依存しないソフトウェアレイヤです。Cisco Secure Firewall の OpenConfig ストリーミング テレメトリ オプションは、gNMI（gRPC ネットワーク管理インターフェイス）プロトコルを使用して、Firewall Threat Defense デバイスからデータ収集システムへのテレメトリストリームを制御および生成できるようにします。

Firewall Threat Defense の正常性ポリシーには、OpenConfig ストリーミングテレメトリ機能をサポートおよび有効化するためのすべての設定が含まれています。正常性ポリシーをデバイスに展開すると、OpenConfig ストリーミングテレメトリ設定によって gNMI サーバーがアクティブ化され、データコレクターからのリモートプロシージャコール（RPC）メッセージのリッスンが開始されます。

OpenConfig ストリーミングテレメトリのサブスクリプションモデル

OpenConfig は、サブスクリプションベースのモデルを使用します。このモデルでは、データコレクターが、Firewall Threat Defense デバイスにテレメトリデータをクエリするか、ストリーミングされるテレメトリデータのコレクターとして動作します。データコレクタは、Firewall Threat Defense デバイスから更新とメトリックを受信する必要がある場合、Firewall Threat Defense gNMI サーバーに subscribeRequest RPC メッセージを送信します。サブスクリプション要求には、データコレクターがサブスクライブする必要がある 1 つ以上のパスの詳細が含まれます。このメッセージには、サブスクリプションの有効期間を示すサブスクリプションモードも含まれます。Firewall Threat Defense サーバーは、次のサブスクリプションモードをサポートしています。

- ワンタイム サブスクリプション（*Once subscription*）：Firewall Threat Defense デバイスは、要求されたデータを gNMI パスに 1 回だけ送信します。
- ストリーミング サブスクリプション（*Stream subscription*）：Firewall Threat Defense は、`SubscribeRequest` RPC メッセージで指定されたトリガーに従って、テレメトリデータを継続的にストリーミングします。
  - サンプリング サブスクリプション（*Sampled subscription*）：Firewall Threat Defense サーバーは、サブスクリプションメッセージで指定された間隔に従って、要求されたデータをストリーミングします。Threat Defense がサポートする最小間隔は 1 分です。

- 変更時サブスクリプション（*On-change subscription*）：Firewall Threat Defense は、要求された値が変化するたびにデータを送信します。

Firewall Threat Defense サーバーは、作成されたサブスクリプションのタイプに従って、データコレクターによって要求された頻度で `SubscribeResponse` RPC メッセージを生成します。

OpenConfig ストリーミングテレメトリの展開モード

OpenConfig ストリーミングテレメトリ設定では、次の展開モードを使用できます。

- **ダイヤルイン（DIAL-IN）**：このモードでは、gNMI サーバーは、Firewall Threat Defense でポートを開き、データコレクターからの `SubscribeRequest` RPC メッセージを待ちます。デバイス正常性ポリシーでは、gNMI サーバーが使用するポート番号と、gNMI サービスに接続できるデータコレクターの IP アドレスを指定できます。指定しない場合、gNMI サーバーは、ポート番号 50051 を使用します。ダイヤルインモードは、テレメトリストリームをサブスクライブするエンドポイントが信頼されている、信頼できるネットワークでの使用に最適です。
- **ダイヤルアウト（DIAL-OUT）**：gNMI サービスは、gNMI データコレクターからのサブスクリプション要求を受け入れてテレメトリデータを提供するサーバーモードで動作するように設計されています。gNMI データコレクターが gNMI サーバーに到達できない場合、Firewall Threat Defense は、トンネルクライアントを使用し、外部サーバーとの gRPC トンネルを確立します。このトンネルにより、gNMI サーバーとクライアントの間での RPC メッセージの交換が可能になります。ダイヤルアウトモードは、データコレクターがクラウド上または信頼できるネットワークの外部でホストされている場合の使用に最適です。

ダイヤルインモードとダイヤルアウトモードのどちらでも、gNMI サーバーと gNMI クライアントの間でのすべての通信で TLS 暗号化が使用されるため、TLS 暗号化用の秘密キーを使用して一連の証明書を生成する必要があります。ダイヤルアウトモードでは、トンネルインフラストラクチャ用の追加のキーが必要です。詳細については、「秘密キーを使用して証明書を生成する方法」を参照してください。

証明書および秘密キーの生成

OpenConfig ストリーミングテレメトリ設定に必要な CA、サーバー、およびクライアント証明書/秘密キーセットを生成します。

（注） 確実に同じ CA を使用して証明書を生成するには、同じエンドポイントから次のコマンドを一緒に実行します。コマンドを再試行する場合は、すべてのコマンドを再試行する必要があります。

始める前に

手順

ステップ 1 次のコマンドを実行するエンドポイントに、フォルダ（keys など）を作成します。

例：

```
mkdir keys
```

ステップ 2 対応する秘密キーを使用して自己署名 CA 証明書を作成します。

例：

次のコマンド例は、新しい RSA 秘密キーを生成し、それを使用して、指定されたサブジェクト情報を含む自己署名 X.509 証明書を作成します。

```
openssl req -x509 -newkey rsa:4096 -days 365 -nodes -keyout keys/ca-key.pem -out
keys/ca-cert.pem -subj "/C=XX
/ST=YY/L=ZZZ/O=Example/OU=EN/CN=gnmi-ca/emailAddress=abc@example.com"
```

件名情報には、指定された国（C）、州（ST）、地域（L）、組織（O）、組織単位（OU）、共通名（CN）、および電子メールアドレスが含まれます。

秘密キーは `ca-key.pem` ファイルとして保存され、証明書は `ca-cert.pem` ファイルとして `keys` フォルダに保存されます。

ステップ 3 指定された共通名（CN）とサブジェクト代替名（SAN）を使用して自己署名サーバー証明書を作成します。

例：

次のコマンド例は、新しい RSA 秘密キーを生成し、それを使用して、指定されたサブジェクト情報を含む自己署名 X.509 証明書を作成します。この例では、192.168.0.200 が Firewall Threat Defense デバイスの IP アドレスであり、192.168.0.202 がクライアントの IP アドレスです。

（注）
この証明書/キーセットをダイヤルインモードで使用する場合、クライアント IP は必要ありません。

```
CN="192.168.0.200"
SAN="IP:192.168.0.200,IP:192.168.0.202"
openssl req -newkey rsa:4096 -nodes -keyout keys/server-key.pem -out keys/server-req.pem
 -subj "/C=XX/ST=YY/L=ZZZ/O=Example/OU=EN/CN=${CN}/emailAddress=abc@example.com}"
openssl x509 -req -extfile <(printf "subjectAltName=${SAN}") -in keys/server-req.pem
-days 60 -CA keys/ca-cert.pem -CAkey keys/ca-key.pem -CAcreateserial -out
keys/server-cert.pem
cat keys/server-key.pem keys/server-cert.pem keys/ca-cert.pem > keys/server-combined.pem
```

`openssl req` コマンドは、新しい RSA 秘密キーと証明書署名要求（CSR）を生成します。秘密キーは `server-key.pem` ファイルとして保存され、CSR は `server-req.pem` ファイルとして `keys` フォルダに保存されます。

`openssl x509` コマンドは、CSR を処理し、サーバー証明書を生成します。サーバー証明書は `server-cert.pem` ファイルとして `keys` フォルダに保存されます。

`cat` コマンドは、サーバーキー、サーバー証明書、およびCA 証明書を `server-combined.pem` という名前の単一のファイルに結合し、そのファイルを keys フォルダに保存します。

Firewall Management Center から **OpenConfig ストリーミングテレメトリ**を設定するときに、`server-combined.pem` をアップロードする必要があります。Firewall Threat Defense およびトンネルサーバー（ダイヤルアウトモード）で動作する gNMI サーバーは、TLS 通信にこの証明書を使用します。パスフレーズを使用して秘密キーを暗号化する場合は、必ず、Firewall Management Center に証明書をアップロードするときにパスフレーズを指定してください。

ステップ 4 指定された共通名（CN）とサブジェクト代替名（SAN）を使用してクライアント証明書を作成します。

例：

次のコマンド例は、新しい RSA 秘密キーを生成し、それを使用して、指定されたサブジェクト情報を含む自己署名 X.509 証明書を作成します。この例では、192.168.0.202 がクライアントの IP アドレスです。

```
CN="192.168.0.202"
SAN="IP:192.168.0.202"
openssl req -newkey rsa:4096 -nodes -keyout keys/client-key.pem -out keys/client-req.pem
 -subj "/C=XX/ST=YY/L=ZZZ/O=example/OU=EN/CN=${CN}/emailAddress=abc@example.com"
openssl x509 -req -extfile <(printf "subjectAltName=${SAN}") -in keys/client-req.pem
-days 60 -CA keys/ca-cert.pem -CAkey keys/ca-key.pem -CAcreateserial -out
keys/client-cert.pem
```

gNMI クライアントは、TLS 通信にクライアント証明書（`client-cert.pem`）と秘密キーを使用します。

ステップ 5 （任意）ダイヤルアウトモードの場合は、指定された共通名（CN）とサブジェクト代替名（SAN）を使用してトンネルサーバー証明書を作成します。

例：

次のコマンド例は、新しい RSA 秘密キーを生成し、それを使用して、指定されたサブジェクト情報を含む自己署名 X.509 証明書を作成します。この例では、192.168.0.202 がクライアントの IP アドレスです。

```
CN="192.168.0.202"
SAN="IP:192.168.0.202"
openssl req -newkey rsa:4096 -nodes -keyout keys/tunnel-server-key.pem -out
keys/tunnel-server-req.pem -subj "
/C=XX/ST=YY/L=ZZZ/O=Example/OU=EN/CN=${CN}/emailAddress=abc@example.com}"
openssl x509 -req -extfile <(printf "subjectAltName=${SAN}") -in keys/tunnel-server-req.pem
 -days 60 -CA keys/ca-cert.pem -CAkey keys/ca-key.pem -CAcreateserial -out
keys/tunnel-server-cert.pem
```

OpenConfig ストリーミングテレメトリの設定

始める前に

- 正常性ポリシー構成を展開する Firewall Threat Defense デバイスで、SSL 証明書と秘密キーのインストールが許可されていることを確認してください。

- OpenConfig ストリーミングテレメトリ実装をサポートする gNMI クライアントを設定していることを確認してください。このクライアントから、Firewall Threat Defense 上の gNMI サーバーに gRPC 要求を行うことができます。
- ダイヤルアウトモードを使用し、OpenConfig ストリーミングテレメトリを設定するために、管理システムで gRPC トンネルサーバーおよびクライアントを設定していることを確認してください。このトンネル設定により、gNMI クライアントと Firewall Threat Defense デバイスが通信できるようになります。
- 次のタスクを実行するには、管理者ユーザーである必要があります。

手順

ステップ 1 **[システム（System）] > [ポリシー（Policy）]**を選択します。

ステップ 2 変更する Threat Defense の正常性ポリシーの横にある [正常性ポリシーの編集（Edit health policy）] アイコンをクリックします。

ステップ 3 [設定（Settings）] タブに移動します。

ステップ 4 [OpenConfigストリーミングテレメトリ（OpenConfig Streaming Telemetry）] スライダを動かして、構成を有効にします。デフォルトでは、この設定は無効になっています。

ステップ 5 [SSL証明書（SSL Certificate）] をアップロードします。gNMI サーバーはこの証明書を使用して、TLS 接続用のサーバー認証を有効にし、チャネルを介したすべての通信を暗号化します。

OpenConfig ストリーミングテレメトリ構成では、PEM 形式の証明書のみサポートされます。Firewall Management Center は、アプライアンスと gNMI コレクタが暗号化通信を接続障害なしで確実に実行できるように、次の証明書検証を実行します。

- ASCII テキストが有効な証明書ファイルであることを確認します。
- アップロードされた証明書の有効期限を確認します。
- アップロードされた PEM ファイルで予期される証明書と秘密キーの数を確認します。ファイルには少なくとも 1 つの証明書が必要であり、証明書内の秘密キーの数は常に 1 である必要があります。
- キーブロックタイプ PRIVATE KEY、RSA PRIVATE KEY、ENCRYPTED PRIVATE KEY、または RSA ENCRYPTED PRIVATE KEY を確認して受け入れます。
- 暗号化された PEM ファイルの場合は、Proc-Type: 4,ENCRYPTED? キーワードが存在することを確認します。
- 暗号化された PEM ファイルに対してパスフレーズが有効であることを確認します。

ステップ 6 （任意）秘密キーファイルが暗号化されている場合は、パスフレーズを指定します。

ステップ 7 gNMI プロトコルを介したテレメトリのストリーミングに使用する展開モードを選択します。

ダイヤルインモードの場合：

1. gNMI サービスのポート番号を割り当てます。

   gNMI サーバーはポートを開き、コレクタからの gRPC 要求を待ちます。

2. Firewall Threat Defense デバイスに接続できる gNMI コレクタの IPv4/IPv6 アドレスを指定します。

3. [コレクタの追加（Add Collector）] をクリックして、gNMI コレクタをさらに追加します。最大 5 つのコレクタを追加できます。

ダイヤルアウトモードの場合：

1. Firewall Threat Defense デバイスからのストリーミングテレメトリをサブスクライブできる gNMI コレクタのホスト名とポート番号を指定します。

2. [コレクタの追加（Add Collector）] をクリックして、gNMI コレクタをさらに追加します。最大 5 つのコレクタを追加できます。

ステップ 8 gNMI コレクタを検証するためのユーザー名とパスワードを指定します。

Firewall Threat Defense サーバーは、`SubscribeRequest` RPC メッセージを受信するときに、このログイン情報を使用して gNMI コレクタを認証します。各テレメトリメッセージは、ユーザー名とパスワードを使用して認証されません。システムは、以前に認証された暗号化されたストリーミングチャネルを使用して、テレメトリメッセージを伝送します。

ステップ 9 [保存（Save）] をクリックします。

次のタスク

構成の変更を有効にするために、正常性ポリシーを Firewall Threat Defense デバイスに展開します。

OpenConfig ストリーミングテレメトリのトラブルシューティング

不明な認証局によって署名された証明書

- Firewall Management Center に正しい証明書をアップロードしたことを確認します。
- 証明書およびキー生成手順を確認します。IP サブジェクト代替名（SAN）が正しく指定されていることを確認します。

証明書が無効

Firewall Management Center に「Request was made for (IP), but the certificate is not valid for (IP)」（（IP）の要求がありましたが、（IP）の証明書が有効ではありません）というエラーが表示される場合は、サーバー証明書およびキー生成手順を確認します。

- サーバー証明書でIP SANが正しく指定されていることを確認します。設定が複数のFirewall Threat Defenseデバイスに適用される場合は、[IP SAN] フィールドですべてのデバイスを指定する必要があります。
- ダイヤルアウトモードを使用している場合は、クライアントIPがサーバー証明書で指定されていることを確認します。

応答オブジェクトの生成に失敗する

「Failed to generate response object, did not receive any data」（応答オブジェクトの生成に失敗し、データを受信しませんでした）というエラーメッセージが表示される場合、gNMI入力プラグインは、メトリックのエクスポートを待機しています。次に、テレグラフの再起動時に表示される応答の例を示します。

```
root@cronserver:/home/secanup/openconfig-test# gnmic -a $ADDRESS:$PORT --tls-cert
$CLIENTCERT --tls-ca $CACERT --tls-key $CLIENTKEY -u $USER -p $PASS sub --mode once
--path "openconfig-system/system/memory"
rpc error: code = Aborted desc = Error in gnmi_server: failed to generate response
object.did not receive any data
Error: one or more requests failed
```

gNMI入力プラグインが再起動するのを待ってから、要求を再試行します。

テレグラフの再起動

テレグラフが応答しない場合は、Firewall Threat DefenseのCLIコンソールで次のコマンドを使用してプロセスを再起動します。

```
pmtool restartbyid hmdaemon
```

gNMI サーバーの現在のステータスの取得

OpenConfigストリーミングテレメトリが有効になっている場合、gNMIサーバーのステータスを確認するには、Firewall Threat DefenseのCLIコンソールを使用して次のコマンドを実行します。

```
curl localhost:9275/OpenConfig/status
```

次に、コマンドへの応答の例を示します。

```
root@firepower:/home/admin# curl localhost:9275/openconfig/status
Mode (Dialin/Dialout): DialIn
Subscription Details:
    Active Subscription Details:
        Stream Mode Subscription Details:
            Total Stream Subscription Request Count: 1
            'Ip of Collector- Subscribe paths:'
                172.16.0.101:45826:
                - /openconfig-system/system/state/hostname
            Sample Subscription Count: 1
            On Change Subscription Count: 0
        Once Mode Subscription Details:
            Total Subscription Request Count: 0
            Total Subscription Count: 0
            'Ip of Collector- Subscribe paths:': {}
    Total Subscription Details:
        Stream Mode Subscription Details:
            Total Stream Subscription Request Count: 1
```

```
        'Ip of Collector- Subscribe paths:':
             172.16.0.101:45826:
             - /openconfig-system/system/state/hostname
    Sample Subscription Count: 1
    On Change Subscription Count: 0
Once Mode Subscription Details:
    Total Subscription Request Count: 0
    Total Subscription Count: 0
    'Ip of Collector- Subscribe paths:': {}
```

ヘルスモニタリングでのデバイスの除外

通常のネットワーク メンテナンスの一環として、アプライアンスを無効にしたり、一時的に使用不能にしたりすることがあります。このような機能停止は意図したものであり、アプライアンスからのヘルス ステータスに Firewall Management Center 上のサマリー ヘルス ステータスを反映させる必要はありません。

ヘルスモニターの除外機能を使用して、アプライアンスまたはモジュールに関するヘルス モニタリング ステータス レポートを無効にすることができます。たとえば、ネットワークのあるセグメントが使用できなくなることがわかっている場合は、そのセグメント上の管理対象デバイスのヘルス モニタリングを一時的に無効にして、Firewall Management Center上のヘルス ステータスにデバイスへの接続がダウンしたことによる警告状態または重大状態が表示されないようにできます。

ヘルス モニタリング ステータスを無効にしても、ヘルス イベントは生成されますが、そのステータスが無効になっているため、ヘルス モニターのヘルス ステータスには影響しません。除外リストからアプライアンスまたはモジュールを削除しても、除外中に生成されたイベントのステータスは [無効（Disabled）] のままです。

アプライアンスからのヘルスイベントを一時的に無効にするには、除外設定ページに移動して、アプライアンスをデバイス除外リストに追加します。設定が有効になると、システムが全体のヘルスステータスを計算するときに、除外されているアプライアンスが考慮されなくなります。[ヘルス モニター アプライアンス ステータスの概要（Health Monitor Appliance Status Summary）] にはこのアプライアンスが [無効（Disabled）] としてリストされます。

個々のヘルスモジュールを無効にすることもできます。たとえば、Firewall Management Center 上でホスト制限に達した場合、ホスト制限ステータスメッセージを無効にできます。個々のインターフェイスのヘルス モジュールの除外は、トランスペアレント モードで動作しているデバイスではサポートされません。

メインの [ヘルスモニター（Health Monitor）] ページで、ステータス行内の矢印をクリックして特定のステータスを持つアプライアンスのリストを展開表示すれば、除外されたアプライアンスを区別できることに注意してください。

（注） Firewall Management Center では、ヘルスモニターの除外設定はローカル構成設定です。そのため、Firewall Management Center 上でデバイスを除外してから削除しても、後で再登録すれば、除外設定は元どおりになります。新たに再登録したデバイスは除外されたままです。

ヘルスモニタリングからのアプライアンスの除外

アプライアンスは個別に、またはグループ、モデル、関連付けられている正常性ポリシーにより、除外できます。

個別のアプライアンスのイベントと正常性ステータスを [無効（Disabled）] に設定する必要がある場合、アプライアンスを除外できます。除外設定が有効になると、アプライアンスが [正常性モニター アプライアンス モジュールの概要（Health Monitor Appliance Module Summary）] に [無効（Disabled）] として表示され、アプライアンスの正常性イベントのステータスが [無効（Disabled）] になります。

手順

ステップ 1 [システム（System）]（⚙）> **[正常性（Health）]** > **[除外（Exclude）]**を選択します。

ステップ 2 [Add Device] をクリックします。

ステップ 3 [デバイスの除外（Device Exclusion）] ダイアログボックスの [使用可能なデバイス（Available Devices）] で、ヘルスモニタリングから除外するデバイスに対して 追加（⊕） をクリックします。

ステップ 4 [除外（Exclude）] をクリックします。選択したデバイスが除外のメインページに表示されます。

ステップ 5 除外リストからデバイスを削除するには、[削除（Delete）]（🗑） をクリックします。

ステップ 6 [適用（Apply）] をクリックします。

次のタスク

アプライアンス上の個別の正常性ポリシーモジュールを除外するには、正常性ポリシーモジュールの除外 （39 ページ）を参照してください。

正常性ポリシーモジュールの除外

アプライアンス上の個別の正常性ポリシーモジュールを除外できます。この操作により、モジュールからの正常性イベントによってアプライアンスのステータスが警告（Warning）または 重大（Critical）に変更されないようにすることができます。

（注） 個々のインターフェイスのヘルス モジュールの除外は、トランスペアレント モードで動作しているデバイスではサポートされません。

除外設定が有効になると、アプライアンスには、ヘルスモニタリングからデバイスで除外されているモジュールの数が表示されます。

ヒント　個別に除外したモジュールを追跡して、必要に応じてそれらを再アクティブ化できるようにしてください。誤ってモジュールを無効にすると、肝要な警告または重大メッセージを見逃す可能性があります。

手順

ステップ 1　[システム（System）]（⚙）>**[正常性（Health）]**>**[除外（Exclude）]**を選択します。

ステップ 2　変更する Firewall Threat Defense デバイスの横にある [編集（Edit）]（✎）をクリックします。

ステップ 3　[正常性モジュールの除外（Exclude Health Modules）] ダイアログボックスでは、デフォルトで、デバイスのすべてのモジュールがヘルスモニタリングから除外されます。一部のモジュールは特定のデバイスにのみ適用できます。詳細は ヘルス モジュール （3 ページ） を参照してください。

ステップ 4　ヘルスモニタリングから除外するモジュールを選択するには、[モジュールレベルの除外の有効化（Enable Module Level Exclusion）] リンクをクリックします。[正常性モジュールの除外（Exclude Health Modules）] ダイアログボックスに、デバイスのすべてのモジュールが表示されます。関連付けられた正常性ポリシーに対応しないモジュールは、デフォルトで無効になります。モジュールを除外するには、次の手順を実行します。

1. 目的のモジュールの横にある [スライダ（Slider）]（⬭）ボタンをクリックします。
2. 選択したモジュールの除外期間を指定するには、[除外期間（Exclude Period）] ドロップダウンリストから期間を選択します。

ステップ 5　（オプション）物理インターフェイスのヘルス ステータスの更新の受信を停止し、代わりにサブインターフェイスのヘルス ステータスに注目するため、物理インターフェイスのヘルス モニタリングを無効にしながら、サブインターフェイスのヘルスアラートをモニターおよび受信できます。

a) まだ有効になっていない場合は、**[インターフェイスの統計情報**（ Interface statistics）] モジュールの横にあるトグルボタンをクリックします。
b) **[除外期間（Exclude Period）]** ドロップダウンリストから、物理インターフェイスのヘルス ステータスが不要な期間を選択します。
c) **[特定のインターフェイスを除外（Exclude specific interfaces）]** オプションボタンをクリックします。
d) 除外する物理インターフェイスの横にあるチェックボックスをオンにします。
e) 物理インターフェイスを選択すると、物理インターフェイスとそのサブインターフェイスのどちらも除外されます。そのため、対応する物理インターフェイスの横にある **[サブインターフェイス（Subinterfaces）]** チェックボックスをオフにして、サブインターフェイスのヘルス アラートを引き続き受信するようにします。

ステップ 6　除外設定の [除外期間（Exclude Period）] で [無期限（Permanent）] 以外を選択した場合は、有効期限が切れたときに設定を自動的に削除することを選択できます。この設定を有効にするに

は、[期限切れの設定の自動削除（Auto-delete expiration configuration）] チェックボックスをオンにします。

ステップ 7 [OK] をクリックします。

ステップ 8 [適用（Apply）] をクリックします。

期限切れの正常性モニターの除外

デバイスまたはモジュールの除外期限が切れた場合、除外をクリアするか更新するかを選択できます。

手順

ステップ 1 [システム（System）]（⚙）> **[正常性（Health）]** > **[除外（Exclude）]**を選択します。

[警告（warning）]（⚠）アイコンがデバイスに対して表示されます。これは、デバイスまたはモジュールをアラートから除外する期間の期限が切れたことを示します。

ステップ 2 デバイスの除外を更新するには、アプライアンスの横にある [編集（Edit）]（✎） をクリックします。[正常性モジュールの除外（Exclude Health Modules）] ダイアログボックスで、[更新（Renew）] リンクをクリックします。デバイスの除外期間が現在の値で延長されます。

ステップ 3 デバイスの除外をクリアするには、アプライアンスの横にある [削除（Delete）]（🗑） をクリックし、[デバイスを除外から削除（Remove the device from exclude）]、[適用（Apply）] の順にクリックします。

ステップ 4 モジュールの除外を更新またはクリアするには、アプライアンスの横にある [編集（Edit）]（✎） をクリックします。[正常性モジュールの除外（Exclude Health Modules）] ダイアログボックスで、[モジュールレベルの除外の有効化（Enable Module Level Exclusion）] リンクをクリックし、モジュールに対して [更新（Renew）] リンクまたは [クリア（Clear）] リンクをクリックします。[更新（Renew）] をクリックすると、モジュールの除外期間が現在の値で延長されます。

ヘルス モニター アラート

正常性ポリシー内のモジュールのステータスが変更された場合に電子メール、SNMP、またはsyslog経由で通知するアラートをセットアップできます。特定のレベルのヘルス イベントが発生したときにトリガーされ警告されるヘルス イベント レベルと、既存のアラート応答を関連付けることができます。

たとえば、アプライアンスがハード ディスク スペースを使い果たす可能性を懸念している場合は、残りのディスク スペースが警告レベルに達したときに自動的に電子メールをシステム管理者に送信できます。ハード ドライブがさらにいっぱいになる場合、ハード ドライブが重大レベルに達したときに 2 つ目の電子メールを送信できます。

ヘルス モニター アラート情報

ヘルス モニタによって生成されるアラートには次の情報が含まれます。

- アラートの重大度レベルを示す [重大度（Severity）]。
- テスト結果がアラートをトリガーとして使用したヘルス モジュールを示す [モジュール（Module）]。
- アラートをトリガーとして使用したヘルス テスト結果を含む [説明（Description）]。

次の表で、これらの重大度レベルについて説明します。

表 *3:* アラートの重大度

重大度	説明
深刻	ヘルス テスト結果がクリティカル アラート ステータスをトリガーとして使用する基準を満たしました。
警告	ヘルス テスト結果が警告アラート ステータスをトリガーとして使用する基準を満たしました。
標準	ヘルス テスト結果が通常のアラート ステータスをトリガーとして使用する基準を満たしました。
エラー（Error）	ヘルス テストが実行されませんでした。
回復済み（Recovered）	ヘルス テスト結果がクリティカルまたは警告のアラート ステータスから通常のアラート ステータスに戻るための基準を満たしました。

ヘルス モニター アラートの作成

この手順を実行するには、管理者ユーザーである必要があります。

ヘルス モニター アラートを作成するときに、シビラティ（重大度）レベル、ヘルス モジュール、およびアラート応答の関連付けを作成します。既存のアラートを使用することも、新しいアラートをシステム ヘルスの報告専用に設定することもできます。選択したモジュールがシビラティ（重大度）レベルに達すると、アラートがトリガーされます。

既存のしきい値と重複するようにしきい値を作成または更新すると、競合が通知されます。重複したしきい値が存在する場合、ヘルス モニターは最も少ないアラートを生成するしきい値を使用し、その他のしきい値を無視します。しきい値のタイムアウト値は、5 ～ 4,294,967,295 分の間にする必要があります。

始める前に

- ヘルス アラートを送信する SNMP、syslog、電子メール サーバーと Firewall Management Center との通信を制御するアラート応答を設定します。Secure Firewall Management Center アラート応答を参照してください。

手順

ステップ 1 [システム（System）]（⚙）>**[正常性（Health）]**>**[モニタアラート（Monitor Alerts）]** を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 [ヘルスアラートの追加（Add Health Alert）] ダイアログボックスの [ヘルスアラート名（Health Alert Name）] フィールドに、ヘルスアラートの名前を入力します。

ステップ 4 [重大度（Severity）] ドロップダウンリストから、アラートをトリガーするために使用する重大度レベルを選択します。

ステップ 5 [アラート（Alert）] ドロップダウンリストから、指定した重大度レベルに達したときにトリガーするアラート応答を選択します。まだアラート応答を構成していない場合は、[アラート（Alerts）] をクリックして [アラート（Alerts）] ページにアクセスし、アラートを設定します。

ステップ 6 [ヘルスモジュール（Health Modules）] リストから、アラートを適用する正常性ポリシーモジュールを選択します。

ステップ 7 オプションで、[しきい値タイムアウト（Threshold Timeout）] フィールドに、それぞれのしきい値期間が終了してしきい値がリセットされるまでの分数を入力します。

ポリシーの実行時間間隔の値がしきい値タイムアウトの値より小さい場合でも、特定のモジュールから報告される 2 つのヘルス イベント間の間隔のほうが常に大きくなります。たとえば、しきい値タイムアウトを 8 分に変更し、ポリシーの実行時間間隔が 5 分である場合、報告されるイベント間の間隔は 10 分（5 × 2）になります。

ステップ 8 [保存（Save）] をクリックして、ヘルス アラートを保存します。

ヘルス モニタ アラートの編集

この手順を実行するには、管理者ユーザーである必要があります。

既存のヘルス モニター アラートを編集して、ヘルス モニター アラートに関連付けられた重大度レベル、ヘルス モジュール、またはアラート応答を変更できます。

手順

ステップ 1 [システム（System）]（⚙）>**[正常性（Health）]**>**[モニタアラート（Monitor Alerts）]**を選択します。

ステップ 2 変更する、必要な正常性アラートに対して表示される [編集（Edit）]（） アイコンをクリックします。

ステップ 3 [正常性アラートの編集（Edit Health Alert）] ダイアログボックスで、[アラート（Alert）] ドロップダウンリストから必要なアラートエントリを選択するか、[アラート（Alerts）] リンクをクリックして新しいアラートエントリを設定します。

ステップ 4 [保存（Save）] をクリックします。

ヘルス モニタ アラートの削除

手順

ステップ 1 [システム（System）]（） > **[正常性（Health）]** > **[モニタアラート（Monitor Alerts）]**を選択します。

ステップ 2 削除する正常性アラートの横にある [削除（Delete）]（） をクリックし、[正常性アラートの削除（Delete health alert）] をクリックして削除します。

次のタスク

- アラートが継続しないようにするには、元になるアラート応答を無効にするか、または削除します。Secure Firewall Management Center アラート応答を参照してください。

ヘルスモニターについて

この手順を実行するには、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 ユーザーである必要があります。

ヘルスモニターには、Firewall Management Center によって管理されているすべてのデバイスに加えて、Firewall Management Center 自体に関して収集されたヘルスステータスが表示されます。ヘルス モニタは以下で構成されています。

- [ヘルスステータス（Health Status）] サマリーページ：Firewall Management Center と Firewall Management Center が管理するすべてのデバイスの正常性を一目で確認できます。マルチドメイン展開では、リーフ ドメインとその親ドメインの両方でデバイスのヘルス ステータスの概要を表示できます。デバイスは、個別に一覧表示されるか、該当する場合は地理位置情報、高可用性、またはクラスタステータスに基づいてグループ化されます。
  - デバイスの正常性を表す六角形にマウスカーソルを合わせると、Firewall Management Center およびデバイスの正常性の概要が表示されます。
  - デバイスの左横にあるドットは、そのデバイスのヘルスを示しています。

- 緑色：アラームなし。
- オレンジ色：少なくとも 1 つのヘルス警告があります。
- 赤色：少なくとも 1 つの重大なヘルスアラームがあります。

- [Monitoring（モニタリング）]ナビゲーションウィンドウ：デバイス階層を移動できます。ナビゲーションペインから個々のデバイスのヘルスモニターを表示できます。

手順

ステップ 1 [システム（System）]（⚙）>**[正常性（Health）]**>**[モニタ（Monitor）]**を選択します。

ステップ 2 [ヘルスステータス（Health Status）] ランディングページで Firewall Management Center とその管理対象デバイスのステータスを確認します。

a) 六角形にポインタを合わせると、デバイスの正常性の概要が表示されます。ポップアップウィンドウに、上位 5 つの正常性アラートの概要の一部が表示されます。ポップアップをクリックすると、正常性アラート概要の詳細ビューが開きます。

b) デバイスリストで[展開（Expand）]（>）と[折りたたみ（Collapse）]（∨）をクリックして、デバイスの正常性アラートのリストを展開または折りたたみます。

行を展開すると、ステータス、タイトル、詳細を含めて、すべての正常性アラートが一覧表示されます。

（注）
正常性アラートは、シビラティ（重大度）レベルでソートされます。

ステップ 3 [Monitoring] ナビゲーションペインを使用して、デバイス固有の正常性モニターにアクセスします。[モニタリング（Monitoring）] ナビゲーションウィンドウを使用する場合：

a) デバイスリストで [展開（Expand）]（>） と [折りたたみ（Collapse）]（∨） をクリックして、管理対象デバイスのリストを展開または折りたたみます。

行を展開すると、すべてのデバイスが一覧表示されます。

b) デバイスをクリックすると、デバイス固有のヘルスモニターが表示されます。

c) ヘルスモニターで、グラフにカーソルを合わせると、グラフ上の特定のポイントでのすべてのメトリックとそれぞれの値が表示されます。グラフをクリックしてメトリック統計ボックスをピン留めすると、メトリックとその値を詳細に調べることができます。統計ボックスを閉じてグラフ上の別のポイントに移動するには、閉じるボタンをクリックします。

次のタスク

- Firewall Management Center によって管理されるデバイスの収集されたヘルスステータスとメトリックについては、デバイスヘルスモニター （50 ページ）を参照してください。

- Firewall Management Center のヘルスステータスについては、Firewall Management Center 正常性モニターの使用 （46 ページ）を参照してください。

  [ホーム（Home）] をクリックすると、いつでも [ヘルスステータス（Health Status）] ランディングページに戻ることができます。

Firewall Management Center 正常性モニターの使用

この手順を実行するには、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 ユーザーである必要があります。

Firewall Management Centerモニターは、Firewall Management Center のヘルスステータスの詳細ビューを提供します。ヘルス モニタは以下で構成されています。

- [高可用性（High Availability）]（設定されている場合）：[高可用性（High Availability）]（HA）パネルには、アクティブユニットとスタンバイユニットのステータス、最終同期時刻、および全体的なデバイスの正常性を含む、現在の HA ステータスが表示されます。
- [イベントレート（Event Rate）]：[イベントレート（Event Rate）] パネルには、ベースラインとしての最大イベントレートと、Firewall Management Center によって受信された全体のイベントレートが表示されます。
- [イベントキャパシティ（Event Capacity）]：[イベントキャパシティ（Event Capacity）] パネルには、イベントカテゴリごとの現在の消費量が表示されます。これには、イベントの保持時間、現在のイベントキャパシティと最大イベントキャパシティ、および Firewall Management Center の設定された最大キャパシティを超えてイベントが保存されたときに警告されるキャパシティ オーバーフロー メカニズムが含まれます。
- [プロセスの正常性（Process Health）]：[プロセスの正常性（Process Health）] パネルには、重要なプロセスの概要ビューと、すべての処理対象の状態（各プロセスの CPU およびメモリ使用率を含む）を表示できるタブがあります。
- [CPU]：[CPU] パネルでは、平均 CPU 使用率（デフォルト）とすべてのコアの CPU 使用率を切り替えることができます。
- [メモリ（Memory）]：[メモリ（Memory）] パネルには、Firewall Management Center での全体のメモリ使用率が表示されます。
- [インターフェイス（Interface）]：[インターフェイス（Interface）] パネルには、すべてのインターフェイスの平均入出力レートが表示されます。
- [ディスク使用率（Disk Usage）]：[ディスク使用率（Disk Usage）] パネルには、ディスク全体の使用状況と、Firewall Management Center データが保存されている重要なパーティションの使用状況が表示されます。
- [ハードウェア統計（Hardware Statistics）]：[ハードウェア統計（Hardware Statistics）] には、Management Center シャーシのファン速度、電源、および温度が表示されます。詳細については、「Management Center のハードウェア統計 （49 ページ）」を参照してください。

ヒント　通常は、非活動状態が 1 時間（または設定された他の時間間隔）続くと、ユーザーはセッションからログアウトされます。ヘルス ステータスを長期間受動的に監視する予定の場合は、一部のユーザーのセッション タイムアウトの免除、またはシステム タイムアウト設定の変更を検討してください。詳細については、内部ユーザーの追加または編集とセッション タイムアウトの設定を参照してください。

手順

ステップ 1　[システム（System）]（⚙）>**[正常性（Health）]**>**[モニタ（Monitor）]** を選択します。

ステップ 2　[モニタリング（Monitoring）] ナビゲーションウィンドウを使用して、Firewall Management Center およびデバイス固有のヘルスモニターにアクセスします。

- スタンドアロン Firewall Management Center は単一のノードとして表示されます。高可用性 Firewall Management Center は、ノードのペアとして表示されます。
- ヘルスモニターは、HA ペアのアクティブとスタンバイ両方の Firewall Management Center に使用できます。そして正常性アラートは、両方のユニットに表示されます。ただし、スタンバイ Firewall Management Center ではさまざまなページへのアクセスが制限される可能性があるため、正常性アラートの解決はアクティブ Firewall Management Center から行う必要があります。

ステップ 3　Firewall Management Center ダッシュボードを確認します。

Firewall Management Center ダッシュボードには、Firewall Management Center の HA 状態の概要ビュー（設定されている場合）と、Firewall Management Center のプロセスとデバイスのメトリック（CPU、メモリ、ディスク使用率など）の概要ビューが含まれています。

アプライアンスのすべてのモジュールの実行

この手順を実行するには、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 ユーザーである必要があります。

ヘルス モジュール テストは、正常性ポリシーの作成時に設定されたポリシー実行時間間隔で自動的に実行されます。ただし、アプライアンスの最新の正常性情報を収集するためにすべてのヘルス モジュール テストをオンデマンドで実行することもできます。

手順

ステップ 1　アプライアンスのヘルスモニターを表示します。

ステップ 2 [すべてのモジュールの実行（Run All Modules）] をクリックします。ステータス バーにテストの進捗状況が表示されてから、[ヘルス モニター アプライアンス（Health Monitor Appliance）] ページが更新されます。

（注）
ヘルス モジュールを手動で実行した場合は、自動的に発生する最初の更新に、手動で実行されたテストの結果が反映されない可能性があります。手動で実行したばかりのモジュールの値が変更されていない場合は、数秒待ってから、デバイス名をクリックしてページを更新します。ページが自動的に再び更新されるまで待機していてもかまいません。

特定のヘルス モジュールの実行

この手順を実行するには、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 ユーザーである必要があります。

ヘルス モジュール テストは、正常性ポリシーの作成時に設定されたポリシー実行時間間隔で自動的に実行されます。ただし、そのモジュールの最新のヘルス情報を収集するためにヘルス モジュール テストをオンデマンドで実行することもできます。

手順

ステップ 1 アプライアンスのヘルスモニターを表示します。

ステップ 2 [モジュール ステータスの概要] グラフで、表示するヘルス アラート ステータス カテゴリの色をクリックします。

ステップ 3 イベントのリストを表示するアラートの [アラート詳細（Alert Detail）] 行で、[実行（Run）] をクリックします。

ステータス バーにテストの進捗状況が表示されてから、[ヘルス モニター アプライアンス（Health Monitor Appliance）] ページが更新されます。

（注）
ヘルス モジュールを手動で実行した場合は、自動的に発生する最初の更新に、手動で実行されたテストの結果が反映されない可能性があります。手動で実行したばかりのモジュールの値が変更されていない場合は、数秒待ってから、デバイス名をクリックしてページを更新します。ページが再び自動的に更新されるまで待機していてもかまいません。

ヘルス モジュール アラート グラフの生成

この手順を実行するには、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 ユーザーである必要があります。

特定のアプライアンスの特定のヘルス テストの一定期間にわたる結果をグラフ化できます。

手順

ステップ 1 アプライアンスのヘルスモニターを表示します。

ステップ 2 [ヘルス モニター アプライアンス（Health Monitor Appliance）] ページの [モジュール ステータスの概要（Module Status Summary）] グラフで、表示するヘルス アラート ステータス カテゴリの色をクリックします。

ステップ 3 イベントのリストを表示するアラートの [アラート詳細（Alert Detail）] 行で、[グラフ（Graph）] をクリックします。

ヒント
イベントが 1 つも表示されない場合は、時間範囲を調整することを考慮してください。

Management Center のハードウェア統計

Management Center アプライアンス（物理のみ）のハードウェア統計には、ファン速度、電源、温度などのハードウェアエンティティに関する情報が含まれます。SNMP でポーリングし、トラップを送信して、Management Center の正常性をモニターするには、次の手順を実行します。

1. MIB をポーリングするために、Management Center で SNMP を有効にします。デフォルトでは、Management Center の SNMP は無効になっています。SNMP ポーリングの設定を参照してください。
2. トラップを有効にするために必要な SNMP ホストごとに ACL エントリを追加します。必ず、ホストの IP アドレスを指定し、ポートとして SNMP を選択してください。アクセスリストの設定を参照してください。

[正常性（Health）] > **[モニター（Monitor）]** ページでハードウェア統計を表示するには、次の手順を実行します。

1. **[正常性（Health）]** > **[ポリシー（Policy）]** ページで、[ハードウェア統計（Hardware Statistics）] モジュールが有効になっていることを確認します。デフォルトのしきい値は変更できます。
2. Management Center の正常性モニタリングダッシュボードにポートレットを追加します。[ハードウェア統計（Hardware Statistics）] メトリックグループを選択し、[ファン速度（Fan Speed）] メトリックと [温度（Temperature）] メトリックを選択してください。

電源のステータスは、**[ヘルスモニタリング（Health Monitoring）]** > **[ホーム（Home）]** ページの Firewall Management Center で確認できます。

（注）

- ファン速度は RPM 単位で表示されます。
- 温度は摂氏単位で表示されます。
- 電源の 1 つのスロットがアクティブである場合、ダッシュボードにはそのスロットが [オンライン（Online）] と表示され、もう 1 つのスロットは [電力なし（No Power）] と表示されます。
- グラフの各水平線は、各 PSU およびファンのステータスをそれぞれ示しています。
- グラフにカーソルを合わせると、個々の統計のデータが表示されます。

デバイスヘルスモニター

デバイスヘルスモニターには、Firewall Management Center によって管理されているすべてのデバイスに関して収集されたヘルスステータスが表示されます。デバイス ヘルス モニターでは、システム イベントを予測して対応するために、Cisco Secure Firewall デバイスのヘルス メトリックが収集されます。デバイスヘルスモニターは、次のコンポーネントで構成されています。

- システムの詳細：インストールされている Cisco Secure Firewall バージョンやその他の展開の詳細などの、管理対象デバイスに関する情報が表示されます。
- トラブルシューティングとリンク：頻繁に使用されるトラブルシューティングのトピックと手順への便利なリンクを提供します。
- ヘルスアラート：ヘルスアラートモニターでは、デバイスの正常性を一目で確認できます。
- 時間範囲：さまざまなデバイス メトリック ウィンドウに表示される情報を制限するための調整可能な時間枠。
- デバイス メトリック：以下を含む、事前定義されたダッシュボード全体で分類されている、一連の主要な ファイアウォール デバイス ヘルス メトリック。
  - CPU：CPU 使用率。プロセス別および物理コア別の CPU 使用率を含みます。
  - Memory：デバイスのメモリ使用率。データプレーンと Snort のメモリ使用率を含みます。
  - Interfaces：インターフェイスのステータスおよび集約トラフィック統計情報。
  - Connections：接続統計（エレファントフロー、アクティブな接続数、ピーク接続数など）および NAT 変換カウント。
  - Snort：Snort プロセスに関連する統計情報。
  - ディスク使用率：パーティションごとのディスクサイズとディスク使用率を含む、デバイスのディスク使用率。

- 重要なプロセス：プロセスの再起動や、CPUやメモリの使用率などのその他の選択されたヘルスモニターを含む、管理対象プロセスに関連する統計。

サポートされているデバイスメトリックの包括的なリストについては、「Cisco Secure Firewall Threat Defense Health Metrics」を参照してください。

システムの詳細の表示とトラブルシューティング

この手順を実行するには、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 ユーザーである必要があります。

[システムの詳細（System Details）]セクションには、選択したデバイスの一般的なシステム情報が表示されます。そのデバイスのトラブルシューティング タスクを起動することもできます。

手順

ステップ 1 [システム（System）]（⚙）>**[正常性（Health）]**>**[モニタ（Monitor）]**を選択します。

[Monitoring] ナビゲーションペインを使用して、デバイス固有の正常性モニターにアクセスします。

ステップ 2 デバイスリストで[展開（Expand）]（>）と[折りたたみ（Collapse）]（∨）をクリックして、管理対象デバイスのリストを展開または折りたたみます。

ステップ 3 デバイスをクリックすると、デバイス固有のヘルスモニターが表示されます。

ステップ 4 [システムとトラブルシューティングの詳細を表示（View System & Troubleshooting Details）]のリンクをクリックします。

このパネルはデフォルトで折りたたまれています。リンクをクリックすると、折りたたまれたセクションが展開され、デバイスの[システムの詳細（System Details）]と[トラブルシューティングとリンク（Troubleshooting & Links）]が表示されます。システムの詳細は次のとおりです。

- **[バージョン（Version）]**：Cisco Secure Firewall ソフトウェアのバージョン。
- [モデル（Model）]：デバイスのモデル。
- [モード（Mode）]：ファイアウォールのモード。Firewall Threat Defense デバイスは、通常のファイアウォール インターフェイスでルーテッド モードとトランスペアレント モードの 2 つのファイアウォール モードをサポートします。
- [VDB]：Cisco 脆弱性データベース（VDB）のバージョン。
- [SRU]：侵入ルールセットのバージョン。
- [Snort]：Snort のバージョン。

ステップ 5 次のトラブルシューティングの選択肢があります。

- トラブルシューティング ファイルを生成します（特定のシステム機能のトラブルシューティング ファイルの生成を参照）。
- 高度なトラブルシューティング ファイルを生成してダウンロードします（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を参照）。
- 正常性ポリシーを作成および変更します（正常性ポリシーの作成（26ページ）を参照）。
- ヘルスモニターアラートを作成および変更します（ヘルス モニター アラートの作成（42ページ）を参照）。

デバイス正常性モニターの表示

この手順を実行するには、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 ユーザーである必要があります。

デバイス正常性モニターには、ファイアウォールデバイスの正常性ステータスの詳細ビューが表示されます。デバイス正常性モニターは、デバイスメトリックをコンパイルし、一連のダッシュボードでデバイスの正常性ステータスとトレンドを提供します。

手順

ステップ 1 [システム（System）]（⚙）>**[正常性（Health）]**>**[モニタ（Monitor）]**を選択します。

[Monitoring] ナビゲーションペインを使用して、デバイス固有の正常性モニターにアクセスします。

ステップ 2 デバイスリストで[展開（Expand）]（>）と[折りたたみ（Collapse）]（∨）をクリックして、管理対象デバイスのリストを展開または折りたたみます。

ステップ 3 ページ上部のデバイス名の右側にあるアラート通知で、デバイスの正常性アラートを確認します。

正常性アラートにポインタを合わせると、デバイスの正常性の概要が表示されます。ポップアップウィンドウに、上位5つの正常性アラートの概要の一部が表示されます。ポップアップをクリックすると、正常性アラート概要の詳細ビューが開きます。

ステップ 4 右上隅のドロップダウンで、時間範囲を設定できます。最短で1時間前（デフォルト）から、最長では2週間前からの期間を反映できます。ドロップダウンから [Custom] を選択して、カスタムの開始日と終了日を設定します。

更新アイコンをクリックして、自動更新を5分に設定するか、自動更新をオフに切り替えます。

ステップ 5 選択した時間範囲について、トレンドグラフの展開オーバーレイの**グラフの最上部に展開の詳細を表示**（⤓）アイコンをクリックします。

アイコンは、選択した時間範囲内の展開数を示します。垂直の帯は、展開の開始時刻と終了時刻を示します。複数の展開の場合、複数の帯または線が表示されることがあります。展開の詳細を表示するには、点線の上部にあるアイコンをクリックします。

ステップ 6 デフォルトでは、デバイスモニターは、いくつかの事前定義されたダッシュボードで正常性およびパフォーマンスのメトリックを報告します。メトリックダッシュボードには次のものが含まれます。

- Overview：CPU、メモリ、インターフェイス、接続統計情報など、他の定義済みダッシュボードからの主要なメトリックを表示します。ディスク使用量と重要なプロセス情報も含まれます。
- CPU：CPU 使用率。プロセス別および物理コア別の CPU 使用率を含みます。
- Memory：デバイスのメモリ使用率。データプレーンと Snort のメモリ使用率を含みます。
- Interfaces：インターフェイスのステータスおよび集約トラフィック統計情報。
- Connections：接続統計（エレファントフロー、アクティブな接続数、ピーク接続数など）および NAT 変換カウント。
- Snort：Snort プロセスに関連する統計情報。
- [ASP Drops]：高速セキュリティパス（ASP）のパフォーマンスと動作に関連する統計情報。

（注）
Firewall Management Center の **[プロセス正常性（Process Health）]** ウィジェットには、各プロセスの CPU 使用率（%）が表示されます。CPU% メトリックは、 Firewall Threat Defense デバイスのコア数に対する使用率を表し、100% は 1 つのコアが完全に使用されていることに対応します。たとえば、8 コアデバイスで 200% の場合、2 つのコアが完全に使用され、6 つのコアが他のプロセスで使用可能です。システムの全体的な CPU 使用率をモニターするには、**[プロセス正常性（Process Health）]** ウィジェットの代わりに **[CPU]** ウィジェットを使用します。

ラベルをクリックすると、さまざまなメトリックダッシュボードに移動できます。サポートされているデバイスメトリックの包括的なリストについては、「Cisco Secure Firewall Threat Defense Health Metrics」を参照してください。

ステップ 7 [新しいダッシュボードの追加（Add New Dashboard）]（＋）をクリックして、使用可能なメトリックグループから独自の変数セットを構成し、カスタム相関ダッシュボードを作成します。デバイスメトリックの相関分析 （53 ページ）を参照してください。

デバイスメトリックの相関分析

デバイス正常性モニターには、システムイベントを予測して対応するのに役立つ、一連の主要 Firewall Threat Defense デバイスメトリックが含まれています。Firewall Threat Defense デバイスの正常性は、これらの報告されたメトリックによって判断できます。

デフォルトでは、デバイスモニターは、いくつかの事前定義されたダッシュボードでこれらのメトリックを報告します。これらのダッシュボードには次のものがあります。

- Overview：CPU、メモリ、インターフェイス、接続統計情報など、他の定義済みダッシュボードからの主要なメトリックを表示します。ディスク使用量と重要なプロセス情報も含まれます。
- CPU：CPU 使用率。プロセス別および物理コア別の CPU 使用率を含みます。
- Memory：デバイスのメモリ使用率。データプレーンと Snort のメモリ使用率を含みます。
- Interfaces：インターフェイスのステータスおよび集約トラフィック統計情報。
- Connections：接続統計（エレファントフロー、アクティブな接続数、ピーク接続数など）および NAT 変換カウント。
- Snort：Snort プロセスに関連する統計情報。
- [ASP Drops]：高速セキュリティパス（ASP）のパフォーマンスと動作に関連する統計情報。

カスタムダッシュボードを追加して、相互に関連するメトリックの相関性を示すことができます。CPU や Snort などの事前定義された相関グループから選択します。または、使用可能なメトリックグループから独自の変数セットを作成して、カスタム相関ダッシュボードを作成します。サポートされているデバイスメトリックの包括的なリストについては、「Cisco Secure Firewall Threat Defense Health Metrics」を参照してください。

始める前に

- ヘルス モニター ダッシュボードで時系列データ（デバイスメトリック）を表示して関連付けるには、REST API を有効にします（**[Settings]** > **[Configuration]** > **[REST API Preferences]**）。
- この手順を実行するには、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 ユーザーである必要があります。

（注） デバイスメトリックの相関分析は、 Firewall Threat Defense 6.7 以降のバージョンでのみ利用可能です。したがって、6.7 以前の Firewall Threat Defense バージョンでは、REST API を有効にしてもヘルス モニタリング ダッシュボードにはこれらのメトリックが表示されません。

手順

ステップ 1 [システム（System）]（⚙） > **[正常性（Health）]** > **[モニタ（Monitor）]** を選択します。

[Monitoring] ナビゲーションペインを使用して、デバイス固有の正常性モニターにアクセスします。

ステップ 2 [デバイス（Devices）] リストで [展開（Expand）]（>）と [折りたたみ（Collapse）]（∨）をクリックして、管理対象デバイスのリストを展開または折りたたみます。

ステップ 3 ダッシュボードを変更するデバイスを選択します。

ステップ 4 [新しいダッシュボードの追加（Add New Dashboard）]（+）アイコンをクリックして、新しいダッシュボードを追加します。

ステップ 5 ダッシュボードを識別する名前を指定します。

ステップ 6 事前定義された相関グループからダッシュボードを作成するには、[事前定義された相関から追加（Add from Predefined Correlations）] ドロップダウンをクリックし、グループを選択して [ダッシュボードの追加（Add Dashboard）] をクリックします。

ステップ 7 カスタム相関ダッシュボードを作成するには、[メトリックグループの選択（Select Metric Group）] ドロップダウンからグループを選択し、[メトリックの選択（Select Metrics）] ドロップダウンから対応するメトリックを選択します。

サポートされているデバイスメトリックの包括的なリストについては、「Cisco Secure Firewall Threat Defense Health Metrics」を参照してください。

ステップ 8 [Add Metrics] をクリックして、別のグループからメトリックを追加して選択します。

ステップ 9 個別のメトリックを削除するには、項目の右側にある [削除（Remove）] ✕ アイコンをクリックします。削除アイコンをクリックしてグループ全体を削除します。

ステップ 10 **[ダッシュボードの追加（Add Dashboard）]** をクリックし、ダッシュボードを正常性モニターに追加します。

ステップ 11 事前定義されたダッシュボードとカスタム相関ダッシュボードは、**編集**または**削除**が可能です。

クラスタのヘルスモニター

Firewall Threat Defense がクラスタの制御ノードである場合、Firewall Management Center はデバイス メトリック データ コレクタからさまざまなメトリックを定期的に収集します。クラスタの ヘルスモニターは、次のコンポーネントで構成されています。

- 概要ダッシュボード：クラスタトポロジ、クラスタ統計、およびメトリックチャートに関する情報を表示します。
  - トポロジセクションには、クラスタのライブステータス、個々の脅威防御の状態、脅威防御ノードのタイプ（制御ノードまたはデータノード）、およびデバイスの状態が表示されます。デバイスの状態は、[無効（Disabled）]（デバイスがクラスタを離れたとき）、[初期状態で追加（Added out of box）]（パブリッククラウドクラスタで Firewall Management Center に属していない追加ノード）、または [標準（Normal）]（ノードの理想的な状態）のいずれかです。
  - クラスタの統計セクションには、CPU 使用率、メモリ使用率、入力レート、出力レート、アクティブな接続数、および NAT 変換数に関するクラスタの現在のメトリックが表示されます。

（注） CPU とメモリのメトリックは、データプレーンと Snort の使用量の個々の平均を示します。

- メトリックチャート、つまり、CPU使用率、メモリ使用率、スループット、および接続数は、指定された期間におけるクラスタの統計を図表で示します。

- 負荷分散ダッシュボード：2 つのウィジェットでクラスタノード全体の負荷分散を表示します。
  - 分布ウィジェットには、クラスタノード全体の時間範囲における平均パケットおよび接続分布が表示されます。このデータは、ノードによって負荷がどのように分散されているかを示します。このウィジェットを使用すると、負荷分散の異常を簡単に特定して修正できます。
  - ノード統計ウィジェットには、ノードレベルのメトリックが表形式で表示されます。クラスタノード全体の CPU 使用率、メモリ使用率、入力レート、出力レート、アクティブな接続数、および NAT 変換数に関するメトリックデータが表示されます。このテーブルビューでは、データを関連付けて、不一致を簡単に特定できます。
- メンバー パフォーマンス ダッシュボード：クラスタノードの現在のメトリックを表示します。セレクタを使用してノードをフィルタリングし、特定ノードの詳細を表示できます。メトリックデータには、CPU使用率、メモリ使用率、入力レート、出力レート、アクティブな接続数、および NAT 変換数が含まれます。
- CCL ダッシュボード：クラスタの制御リンクデータ、つまり入力レートと出力レートをグラフ形式で表示します。
- トラブルシューティングとリンク：頻繁に使用されるトラブルシューティングのトピックと手順への便利なリンクを提供します。
- 時間範囲：さまざまなクラスタ メトリック ダッシュボードやウィジェットに表示される情報を制限するための調整可能な時間枠。
- カスタムダッシュボード：クラスタ全体のメトリックとノードレベルのメトリックの両方に関するデータを表示します。ただし、ノードの選択は脅威防御メトリックにのみ適用され、ノードが属するクラスタ全体には適用されません。

クラスタのヘルスモニターの表示

この手順を実行するには、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 ユーザーである必要があります。

クラスタヘルスモニターは、クラスタとそのノードのヘルスステータスの詳細なビューを提供します。このクラスタヘルスモニターは、一連のダッシュボードでクラスタのヘルスステータスと傾向を提供します。

始める前に

- Firewall Management Center の 1 つ以上のデバイスからクラスタを作成しているかを確認します。

手順

ステップ 1 [システム（System）]（⚙）>**[正常性（Health）]**>**[モニタ（Monitor）]** を選択します。

[モニタリング（Monitoring）] ナビゲーションウィンドウを使用して、ノード固有のヘルスモニターにアクセスします。

ステップ 2 デバイスリストで [展開（Expand）]（>）と [折りたたみ（Collapse）]（∨）をクリックして、管理対象のクラスタデバイスのリストを展開または折りたたみます。

ステップ 3 クラスタのヘルス統計を表示するには、クラスタ名をクリックします。デフォルトでは、クラスタモニターは、いくつかの事前定義されたダッシュボードで正常性およびパフォーマンスのメトリックを報告します。メトリックダッシュボードには次のものが含まれます。

- [概要（Overview）]：他の事前定義されたダッシュボードからの主要なメトリックを表示します。ノード、CPU、メモリ、入力レート、出力レート、接続統計情報、NAT 変換情報などが含まれます。
- [負荷分散（Load Distribution）]：クラスタノード間のトラフィックとパケットの分散。
- [メンバーパフォーマンス（Member Performance）]：CPU 使用率、メモリ使用率、入力スループット、出力スループット、アクティブな接続、および NAT 変換に関するノードレベルの統計情報。
- [CCL]：インターフェイスのステータスおよび集約トラフィックの統計情報。

ラベルをクリックすると、さまざまなメトリックダッシュボードに移動できます。サポートされているクラスタメトリックの包括的なリストについては、「Cisco Secure Firewall Threat Defense Health Metrics」を参照してください。

ステップ 4 右上隅のドロップダウンで、時間範囲を設定できます。最短で 1 時間前（デフォルト）から、最長では 2 週間前からの期間を反映できます。ドロップダウンから [Custom] を選択して、カスタムの開始日と終了日を設定します。

更新アイコンをクリックして、自動更新を 5 分に設定するか、自動更新をオフに切り替えます。

ステップ 5 選択した時間範囲について、トレンドグラフの展開オーバーレイの展開アイコンをクリックします。

展開アイコンは、選択した時間範囲内の展開数を示します。垂直の帯は、展開の開始時刻と終了時刻を示します。複数の展開の場合、複数の帯または線が表示されます。展開の詳細を表示するには、点線の上部にあるアイコンをクリックします。

ステップ 6 （ノード固有のヘルスモニターの場合）ページ上部のデバイス名の右側にあるアラート通知で、ノードの正常性アラートを確認します。

正常性アラートにポインタを合わせると、ノードの正常性の概要が表示されます。ポップアップウィンドウに、上位5つの正常性アラートの概要の一部が表示されます。ポップアップをクリックすると、正常性アラート概要の詳細ビューが開きます。

ステップ 7 （ノード固有のヘルスモニターの場合）デフォルトでは、デバイスモニターは、いくつかの事前定義されたダッシュボードで正常性およびパフォーマンスのメトリックを報告します。メトリックダッシュボードには次のものが含まれます。

- Overview：CPU、メモリ、インターフェイス、接続統計情報など、他の定義済みダッシュボードからの主要なメトリックを表示します。ディスク使用量と重要なプロセス情報も含まれます。
- CPU：CPU 使用率。プロセス別および物理コア別の CPU 使用率を含みます。
- Memory：デバイスのメモリ使用率。データプレーンと Snort のメモリ使用率を含みます。
- Interfaces：インターフェイスのステータスおよび集約トラフィック統計情報。
- Connections：接続統計（エレファントフロー、アクティブな接続数、ピーク接続数など）および NAT 変換カウント。
- [Snort]：Snort プロセスに関連する統計情報。
- [ASP ドロップ（ASP drops）]：さまざまな理由でドロップされたパケットに関連する統計情報。

ラベルをクリックすると、さまざまなメトリックダッシュボードに移動できます。サポートされているデバイスメトリックの包括的なリストについては、「Cisco Secure Firewall Threat Defense Health Metrics」を参照してください。

ステップ 8 正常性モニターの右上隅にあるプラス記号[新しいダッシュボードの追加（Add New Dashboard）]（＋）をクリックして、使用可能なメトリックグループから独自の変数セットを構成し、カスタムダッシュボードを作成します。

クラスタ全体のダッシュボードの場合は、クラスタのメトリックグループを選択してから、メトリックを選択します。

ヘルス モニター ステータスのカテゴリ

使用可能なステータス カテゴリを、シビラティ（重大度）別に次の表に示します。

表 *4:* ヘルス ステータス インジケータ

ステータス レベル	ステータス アイコン	円グラフのステータスの色	説明
エラー（Error）	**エラー**（  ）	黒色	アプライアンス上の 1 つ以上のヘルス モニタリング モジュールで障害が発生し、それ以降、正常に再実行していないことを示します。テクニカル サポート担当者に連絡して、ヘルス モニタリング モジュールの更新プログラムを入手してください。
クリティカル	[クリティカル（Critical）]（）	赤	アプライアンス上の1つ以上のヘルス 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。
警告	[警告（warning）]（）	黄	アプライアンス上の1つ以上のヘルス 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。 このステータスは、デバイス構成の変更が原因で、必要なデータが一時的に利用できないか処理できなかったという過渡的な状態も示しています。モニタリングサイクルに応じて、この過渡状態は自動修正されます。
通常	[標準（Normal）]（）	グリーン	アプライアンス上のすべてのヘルス モジュールがアプライアンスに適用された正常性ポリシーで設定された制限内で動作していることを示します。
Recovered	[回復済み（Recovered）]（）	緑	アプライアンス上のすべてのヘルス モジュールがアプライアンスに適用された正常性ポリシーで設定された制限内で動作していることを示します。これには、前に Critical または Warning 状態だったモジュールも含まれます。
無効	**無効**（）	青	アプライアンスが無効または除外されている、アプライアンスに正常性ポリシーが適用されていない、またはアプライアンスが現在到達不能になっていることを示します。

ヘルス イベント ビュー

[ヘルス イベント ビュー（Health Event View）] ページでは、ヘルス モニタがログに記録したヘルス イベントを、Firewall Management Center ログ ヘルス イベントで表示できます。完全に

カスタマイズ可能なイベント ビューを使用すれば、ヘルス モニタによって収集されたヘルス ステータス イベントを迅速かつ容易に分析できます。イベント データを検索して、調査中のイベントに関係する可能性のある他の情報に簡単にアクセスしたりできます。ヘルス モジュールごとにテストされる条件を理解していれば、ヘルス イベントに対するアラートをより効率的に設定できます。

ヘルス イベント ビュー ページで多くの標準イベント ビュー機能を実行できます。

ヘルス イベントの表示

この手順を実行するには、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 ユーザーである必要があります。

[ヘルス イベントのテーブル ビュー（Table View of Health Events）] ページには、指定したアプライアンス上のすべてのヘルス イベントのリストが表示されます。

Firewall Management Center 上の [ヘルス モニター（Health Monitor）] ページからヘルス イベントにアクセスした場合は、すべての管理対象アプライアンスのすべてのヘルス イベントが表示されます。

ヒント このビューをブックマークすれば、イベントの [ヘルス イベント（Health Events）] テーブルを含むヘルス イベント ワークフロー内のページに戻ることができます。ブックマークしたビューには、現在見ている時間範囲内のイベントが表示されますが、必要に応じて時間範囲を変更してテーブルを最新情報で更新することができます。

手順

[システム（System）]（⚙） > **[正常性（Health）]** > **[イベント（Events）]**を選択します。

ヒント
ヘルス イベントのテーブル ビューが含まれていないカスタム ワークフローを使用している場合は、[(ワークフローの切り替え)（(switch workflow)）] をクリックします。[ワークフローの選択（Select Workflow）] ページで、[ヘルス イベント（Health Events）] をクリックします。

（注）
イベントが 1 つも表示されない場合は、時間範囲を調整することを考慮してください。

モジュール/アプライアンス別のヘルス イベントの表示

手順

ステップ 1 アプライアンスのヘルス モニターを表示します（デバイス正常性モニターの表示 （52 ページ）を参照）。

ステップ 2 [モジュール ステータスの概要（Appliance Status Summary）] グラフで、表示するイベント ステータス カテゴリの色をクリックします。

[アラート詳細（Alert Detail）] リストで、表示を切り替えてイベントを表示または非表示にします。

ステップ 3 イベントのリストを表示するアラートの [アラート詳細（Alert Detail）] 行で、[イベント（Events）] をクリックします。

[ヘルス イベント（Health Events）] ページが開いて、制限としてアプライアンスの名前と指定したヘルス アラート モジュールの名前を含むクエリーの結果が表示されます。イベントが 1 つも表示されない場合は、時間範囲を調整することを考慮してください。

ステップ 4 指定したアプライアンスのすべてのステータスイベントを表示する場合は、[検索制約（Search Constraints）] を展開し、[モジュール名（Module Name）] 制限をクリックして削除します。

ヘルス イベント テーブルの表示

ヘルスイベントテーブルを表示および変更できます。

手順

ステップ 1 [システム（System）]（⚙） > **[正常性（Health）]** > **[イベント（Events）]**を選択します。

ステップ 2 次の選択肢があります。

- ブックマーク：すぐに現在のページに戻れるように、現在のページをブックマークするには、[このページのブックマーク（Bookmark This Page）] をクリックしてブックマークの名前を指定し、[保存（Save）] をクリックします。
- ワークフローの変更：別のヘルスイベントワークフローを選択するには、[(ワークフローの切り替え)（(switch workflow)）] をクリックします。
- イベントの削除：ヘルスイベントを削除するには、削除するイベントの横にあるチェックボックスをオンにして、[削除（Delete）] をクリックします。現在の制約されているビューですべてのイベントを削除するには、[すべて削除（Delete All）] をクリックしてから、すべてのイベントを削除することを確認します。
- レポートの生成：テーブル ビューのデータに基づいてレポートを生成するには、[レポート デザイナ（Report Designer）] をクリックします。

- 変更：ヘルス テーブル ビューに表示されるイベントの時刻と日付範囲を変更します。イベント ビューを時間で制約している場合は、（グローバルであるかイベントに特有であるかに関係なく）アプライアンスに設定されている時間枠の範囲外に生成されたイベントがイベント ビューに表示されることがあることに注意してください。アプライアンスに対してスライドする時間枠を設定した場合でも、この状況が発生することがあります。
- 移動：イベント ビュー ページを使用して移動します。
- ブックマークの移動：ブックマーク管理ページに移動するには、任意のイベント ビューから [ブックマークの表示（View Bookmarks）] をクリックします。
- その他に移動：他のイベント テーブルに移動して関連イベントを表示します。
- ソート：表示されたイベントをソートする、イベント テーブルに表示するカラムを変更する、または表示するイベントを制約します。
- すべて表示：すべてのイベントのイベントの詳細をビューに表示するには、[すべて表示（View All）] をクリックします。
- 詳細の表示：単一のヘルス イベントに関連付けられる詳細を表示するには、イベントの左側にある下矢印のリンクをクリックします。
- 複数表示：複数のヘルス イベントのイベント詳細を表示するには、詳細を表示するイベントに対応する行の横にあるチェックボックスをオンにして、[表示（View）] をクリックします。
- ステータスの表示：特定のステータスのすべてのイベントを表示するには、そのステータスのイベントの [ステータス（Status）] 列のステータスをクリックします。

[ヘルス イベント（Health Events）] テーブル

正常性ポリシー内で有効にされたヘルス モニター モジュールが、さまざまなテストを実行してアプライアンスのヘルス ステータスを特定します。ヘルス ステータスが指定された基準を満たしている場合は、ヘルス イベントが生成されます。

次の表で、ヘルス イベント テーブルで表示および検索できるフィールドについて説明します。

表 *5:* ヘルス イベント フィールド

フィールド	説明
Module Name	表示するヘルス イベントを生成したモジュールの名前を指定します。たとえば、CPU パフォーマンスを測定するイベントを表示するには、「CPU」と入力します。検索によって、該当する CPU 使用率イベントと CPU 温度イベントが取得されます。
テスト名（Test Name） （検索専用）	イベントを生成したヘルス モジュールの名前。

フィールド	説明
時刻（Time） （検索専用）	ヘルス イベントのタイムスタンプ。
Description	イベントを生成したヘルスモジュールの説明。たとえば、プロセスが実行できない場合に生成されるヘルス イベントには [Unable to Execute] というラベルが付けられます。
Value	イベントが生成されたヘルス テストから得られた結果の値（単位数）。 たとえば、モニター対象デバイスが 80% 以上の CPU リソースを使用しているときに生成されるヘルス イベントをFirewall Management Centerが生成した場合の値は 80 ～ 100 です。
単位	結果の単位記述子。アスタリスク（*）を使用してワイルドカード検索を作成できます。 たとえば、モニター対象デバイスが 80% 以上の CPU リソースを使用しているときに生成されるヘルス イベントをFirewall Management Centerが生成した場合の単位記述子はパーセント記号（%）です。
Status	アプライアンスに報告されるステータス（[クリティカル（Critical）]、[黄色（Yellow）]、[緑色（Green）]、または [無効（Disabled）]）。
Device	ヘルス イベントが報告されたアプライアンス。

ヘルス モニタリングの履歴

表 *6*：

機能	最小 **Firewall Management Center**	最小 **Firewall Threat Defense**	詳細
証明書の有効期限が近づいたときにアラートを受信します。	7.7.0	いずれか	Firewall Management Center および Firewall Threat Defense デバイスで使用されるサービス認証証明書の有効期限をモニターし、証明書の有効期限が近づいたときに事前にアラートを受け取ることができるようになりました。この機能は、期限切れが近づいている証明書を特定するのに役立ちます。これにより、証明書を事前に更新して、予期しないサービスの中断を防ぐことができます。 証明書モニタリング機能を有効にするには、[システム（System）]（⚙）>**[ポリシー（Policy）]** を選択し、正常性ポリシーの横にある [編集（Edit）]（✎）アイコンをクリックして、[証明書モニタリング（Certificate Monitoring）] モジュールを有効にします。

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
イベントデータベースのモニタ	7.7.0	いずれか	Firewall Management Center は、ファイアウォール イベントおよび接続サマリーなどのイベント関連データに MonetDB データベースを使用します。新しい MonetDB 統計正常性モジュールは、データベース サイズ、アクティブな接続、メモリ使用量など、正常性モニターでも確認できるデータベース統計を収集します。 トラブルシューティングのベストプラクティスは、このモジュールを有効のままにすることです。 新規/変更された画面：**[システム（System）]** > **[正常性（Health）]** > **[ポリシー（Policy）]**。
リーフドメインとその親ドメインの両方でデバイスの正常性ステータス概要を表示します	7.6.1	任意	マルチドメイン展開では、リーフ ドメインとその親ドメインの両方でデバイスのヘルス ステータスの概要を表示できます。
デフォルトの正常性ポリシーの設定	7.6.0	任意（Any）	ユーザーが作成した正常性ポリシーをデフォルトの正常性ポリシーとして設定できるようになりました。デバイスを Management Center に追加すると、Management Center は管理対象デバイスにデフォルトの正常性ポリシーを適用します。 デフォルトの正常性ポリシーを設定するには、[システム（System）]（⚙）>**[ポリシー（Policy）]**を選択し、デフォルトとして設定する正常性ポリシーの横にある [その他のアクション（More Actions）]（⋮）アイコンをクリックし、[デフォルトに設定（Set as Default）] をクリックします。
正常性ポリシーをカスタマイズして、データの収集を継続しながら正常性アラートを最小限に抑えます。	7.6.0	任意（Any）	データ収集を停止することなく、CPU、メモリ、および ASP ドロップ正常性モジュール内の個々の属性の正常性アラートを無効化にできるようになりました。特定の属性の正常性アラートを無効にすることで、正常性アラートのノイズを最小限に抑え、最も重大な問題に集中できます。 新規/変更された画面：**[システム（System）]** > **[正常性（Health）]** > **[ポリシー（Policy）]**をクリックし、**[Firewall Threat Defense 正常性ポリシー（Firewall Threat Defense health policy）]** または **[Firewall Management Center 正常性ポリシー（Firewall Management Center health policy）]** の横にある **[編集（Edit）]** アイコンをクリックします。
Talos 接続の正常性アラート	7.6.0	7.6.0	指定された期間内に Talos 接続デーモンがその正常性ステータスを報告しなかった場合に、Management Center がアラートを発するようになりました。

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
Firewall Management Center メモリ使用量モジュールのデフォルトのしきい値を更新しました。	7.4.1	任意	Management Center のメモリ使用量の警告と重大アラームのデフォルトのしきい値が、それぞれ 88% と 90% に設定されました。 新規/変更された画面：**[システム（System）]** > **[正常性（Health）]** > **[ポリシー（Policy）]** > では、**[Firewall Management Center 正常性ポリシー（Firewall Management Center Health Policy）]** > **[正常性モジュール（Health Modules）]** > **[メモリ使用量（Memory Usage）]**を編集します。
Firewall Management Center のメモリ使用量の計算が改善されました。	7.4.1	任意	Management Center のメモリ使用量モジュールは、メモリ使用量を計算するときに使用可能なスワップメモリとキャッシュメモリの量を考慮して、メモリ使用量を正確に判断し、正常性アラートを送信します。 新規/変更された画面：**[システム（System）]** > **[正常性（Health）]** > **[モニター（Monitor）]** > **[Firewall Management Center]** > **[新しいダッシュボードの追加（Add New Dashboard）]**。
NTP サーバーの同期の問題に関する正常性アラート。	7.4.1	任意	Cisco Secure Firewall Management Center の正常性ポリシーに **Time Sever Status** モジュールが導入されました。有効にすると、このモジュールは NTP サーバーの設定をモニターし、NTP サーバーが使用できない場合、または NTP サーバーの設定が無効な場合にアラートを出します。 新規/変更された画面：**[システム（System）]** > **[正常性（Health）]** > **[ポリシー（Policy）]** > **[Firewall Management Center 正常性ポリシー（Firewall Management Center Health Policy）]** > **[正常性モジュール（Health Modules）]** > **[時刻の同期（Time Synchronization）]**。
Firepower 1010 および 1100 デバイスの、CPU およびシャーシの温度アラート。	7.4.1	7.4.1	Firepower 1010 および 1100 デバイスについて、CPU またはシャーシの温度に関する警告または重大レベルのアラートが Management Center に表示されます。
OpenConfig を使用して、テレメトリを外部サーバーにストリーミング。	7.4	7.4	OpenConfig を使用して、メトリックとヘルスモニタリング情報を Threat Defense デバイスから外部サーバー（gNMI コレクタ）に送信できるようになりました。TLS により暗号化された接続を開始するように Threat Defense またはコレクタを設定できます。 新規/変更された画面：**[システム（System）]** > **[正常性（Health）]** > **[ポリシー（Policy）]** > **[Firewall Threat Defenseポリシー（Firewall Threat Defense Policies）]** > **[設定（Settings）]** > **[OpenConfig ストリーミングテレメトリ（OpenConfig Streaming Telemetry）]**。

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
ヘルスモニターの使いやすさの強化。	7.4	いずれか	カスタムダッシュボードを簡単に作成できる [新しいダッシュボードの追加（Add New Dashboard）] ダイアログボックスの改善。事前定義された Device Health 監視ダッシュボードを編集または削除するオプションが含まれています。 新規/変更された画面：**[システム（System）]** > **[ヘルス（Health）]** > **[モニタ（Monitor）]** > **[デバイス]** > **[新しいダッシュボードを追加（Add New Dashboard）]**。
新しいクラスタヘルスモニターダッシュボード。	7.3	任意（Any）	クラスタヘルスモニターメトリックを表示するための新しいダッシュボードが、次のコンポーネントで導入されました。 • [概要（Overview）]：クラスタトポロジ、クラスタ統計、およびメトリックチャートに関する情報を表示します。 • [負荷分散（Load Distribution）]：クラスタノード間の負荷分散を表示します。 • [メンバーパフォーマンス（Member Performance）]：クラスタのすべてのメンバーノードの現在のメトリックを表示します。 • [CCL]：クラスタの制御リンクデータ、つまり入力レートと出力レートをグラフ形式で表示します。 **（注）** これらの機能は、クラスタでのみ使用できます。したがって、クラスタダッシュボードを表示して使用するには、[モニタリング（Monitoring）] ペインの [デバイス（Devices）] リストでクラスタを選択する必要があります。 新規/変更された画面：**[システム（System）]** > **[正常性（Health）]** > **[モニター（Monitor）]**。

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
新しいハードウェア統計モジュール。	7.3	任意（Any）	Firewall Management Center ハードウェアと環境のステータス統計がヘルス モニター ダッシュボードに追加されました。 • Management Center ハードウェアでハードウェアデーモンのモニタリングを有効にするために、新しいポリシーモジュールである [ハードウェア統計（Hardware Statistics）] が導入されました。メトリックには、ファン速度、温度、および電源が含まれました。 • モニタリングダッシュボードにハードウェアの正常性メトリックをグラフィカルに表示するためのカスタムメトリックグループの [ハードウェア統計（Hardware Statistics）] も追加されました。 • 電源ステータスは、Management Center の**正常性アラート**でキャプチャされます。 （注） これらの機能は、Management Center にのみ適用されるため、Management Center ダッシュボードでのみ使用できます。 新規/変更された画面： • **[システム（System）] > [正常性（Health）] > [モニター（Monitor）]** • **[システム（System）] > [正常性（Health）] > [ポリシー（Policy）]**

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
新しいハードウェアと環境のステータス メトリック グループ。	7.3	任意（Any）	Threat Defense ハードウェアと環境のステータス統計がヘルス モニター ダッシュボードに追加されました。 • Threat Defense に関するハードウェア関連の統計情報を表示するために、カスタムメトリックグループの [ハードウェア/環境ステータス（Hardware / Environment Status）] が導入されました。メトリックには、ファン速度、シャーシ温度、SSD ステータス、および電源が含まれました。 • デバイスの**正常性アラート**が拡張され、Threat Defense ハードウェアの電源ステータスが含まれるようになりました。異常な温度ステータスの場合は重大アラートが表示され、通常の温度ステータスの場合は正常アラートが表示されます。 （注） これらの機能は、Threat Defense でのみ使用できます。したがって、[モニタリング（Monitoring）] ペインの [デバイス（Devices）] リストで適切なデバイスを選択する必要があります。 新規/変更された画面：**[システム（System）] > [正常性（Health）] > [モニター（Monitor）]**。
デバイス設定履歴ファイルのサイズに関する正常性アラート	7.2.6	いずれか	Firewall Management Center 上のデバイス設定履歴ファイルのサイズが許容制限サイズを超えると、[ディスク使用量（Disk Usage）] モジュールから正常性アラートが送信されます。このアラートは、デフォルトで有効になっています。 Secure Firewall Management Center バージョン 7.3.0 および 7.4.0 では、構成バージョンのサイズを超過した場合の正常性アラートはサポートされていません。

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
ヘルスモニターの使いやすさの強化。	7.1	任意（Any）	次の UI ページが改善され、データの使いやすさとプレゼンテーションが向上しました。 • ポリシー（Policy） • 除外（Exclude） • モニターアラート 新規/変更された画面： • **[システム（System）] > [正常性（Health）] > [ポリシー（Policy）]** • **[システム（System）] > [正常性（Health）] > [除外（Exclude）]** • **[システム（System]） > [正常性（Health）] > [モニター アラーと（Monitor Alerts）]**
エレファントフローの検出。	7.1	任意（Any）	ヘルスモニターには、次の拡張機能が含まれます。 • 接続統計情報には、アクティブなエレファントフローが含まれます。 • 接続グループメトリックには、アクティブなエレファントフローの数が含まれます。 エレファントフロー検出機能は、Cisco Firepower 2100 シリーズではサポートされていません。
アンマネージドディスク使用率が高いアラートは廃止されました。	7.0.6	任意（Any）	ディスク使用状況モジュールは、管理対象外のディスク使用率が高い場合にアラートを出さなくなりました。アップグレード後も、正常性ポリシーを管理対象デバイスに展開する（アラートの表示を停止する）か、デバイスをアップグレードする（アラートの送信を停止する）まで、これらのアラートが表示され続ける場合があります。 **（注）** バージョン 7.0 ～ 7.0.5、7.1.x、7.2.0 ～ 7.2.3、および 7.3.x は、引き続きこれらのアラートをサポートします。Firewall Management Center がこれらのバージョンのいずれかを実行している場合、アラートが引き続き表示される場合があります。

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
新しいヘルス モジュール。	7.0	任意（Any）	

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
			次の正常性モジュールが追加されました。 • [Cisco Advanced Malware Protection接続ステータス（AMP Connection Status）]：Firewall Threat Defense からの Cisco Advanced Malware Protection クラウド接続をモニターします。 • [AMP Threat Gridのステータス（AMP Threat Grid Status）]：Firewall Threat Defense からの AMP Threat Grid クラウド接続をモニターします。 • [ASPドロップ（ASP Drop）]：データプレーンの高速セキュリティパスによってドロップされた接続をモニターします。 • [高度なSnort統計情報（Advanced Snort Statistics）]：パケットパフォーマンス、フローカウンタ、およびフローイベントに関連する Snort 統計情報をモニターします。 • [イベントストリームステータス（Event Stream Status）]：イベントストリーマを使用するサードパーティ製クライアント アプリケーションへの接続をモニターします • [FMCアクセス設定の変更（FMC Access Configuration Changes）]：Firewall Management Center で直接加えられたアクセス設定の変更をモニターします。 • [FMC HAステータス（FMC HA Status）]：アクティブおよびスタンバイ Firewall Management Center と、デバイス間の同期ステータスをモニターします。[HAステータス（HA Status）] モジュールと置き換わります。 • [FTD HAステータス（FTD HA Status）]：アクティブおよびスタンバイ Firewall Threat Defense HA ペアと、デバイス間の同期ステータスをモニターします。 • [ファイルシステム整合性チェック（File System Integrity Check）]：システムで CC モードまたは UCAPL モードが有効になっている場合、ファイルシステム整合性チェックを実行します。 • [フローオフロード（Flow Offload）]：Firepower 9300 および 4100 プラットフォームのハードウェア フロー オフロード統計をモニターします。 • [ヒットカウント（Hit Count）]：アクセス コントロール ポリシーで特定のルールがヒットした回数をモニターします。 • [MySQLのステータス（MySQL Status）]：MySQL データベースの

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
			ステータスをモニターします。 • [NTPステータスFTD（NTP Status FTD）]：管理対象デバイスの NTP クロック同期ステータスをモニターします。 • [RabbitMQステータス（RabbitMQ Status）]：RabbitMQ メッセージングブローカのステータスをモニターします。 • [ルーティング統計情報（Routing Statistics）]：Firewall Threat Defense からの IPv4 と IPv6 の両方のルート情報をモニターします。 • [セキュリティサービス交換接続ステータス（Security Services Exchange Connection Status）]：Firewall Threat Defense からのセキュリティサービス交換クラウド接続をモニターします。 • [Sybaseのステータス（Sybase Status）]：Sybase データベースのステータスをモニターします。 • [未解決グループモニター（Unresolved Groups Monitor）]：アクセス コントロール ポリシーで使用される未解決グループをモニターします。 • [VPN統計（VPN Statistics）]：サイト間およびリモートアクセスの VPN トンネルの統計をモニターします。 • [xTLSカウンタ（xTLS Counters）]：xTLS/SSL フロー、メモリ、およびキャッシュの有効性をモニターします。

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
ヘルスモニターの機能拡張。	7.0	任意（Any）	ヘルスモニターには、次の機能拡張が追加されています。 • 次の概要ビューを備え、機能強化された Firewall Management Center ダッシュボード： • ハイ アベイラビリティ • イベントレートとキャパシティ • プロセスの正常性 • CPU しきい値 • メモリ • インターフェイスレート • ディスク使用率（Disk Usage） • 機能強化された Firewall Threat Defense ダッシュボード： • スプリットブレインシナリオのヘルスアラート • 新しいヘルスモジュールから使用できる追加のヘルスメトリック

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
新しいヘルス モジュール。	6.7	いずれか	[CPU使用率（CPU Usage）] モジュールは使用されなくなりました。CPU 使用率については、代わりに次のモジュールを参照してください。 • CPU使用率（コアごと）：すべてのコアのCPU使用率をモニターします。 • CPU使用率データプレーン：デバイス上のすべてのデータプレーンプロセスの平均 CPU 使用率をモニターします。 • CPU 使用率 Snort：デバイス上の Snort プロセスの平均 CPU 使用率をモニターします。 • CPU使用率システム：デバイス上のすべてのシステムプロセスの平均 CPU 使用率をモニターします。 統計情報を追跡するために、次のモジュールが追加されました。 • [接続統計情報（Connection Statistics）]：接続統計情報と NAT 変換カウントをモニターします。 • クリティカルプロセス統計情報：クリティカルプロセスの状態、リソース消費量、再起動回数をモニターします。 • 展開された設定の統計情報：展開された設定に関する統計情報（ACE の数や IPS ルールなど）をモニターします。 • [Snort統計情報（Snort Statistics）]：イベント、フロー、およびパケットの Snort 統計情報をモニターします。 メモリ使用率を追跡するために、次のモジュールが追加されました。 • [メモリ使用率データプレーン（Memory Usage Data Plane）]：データプレーンプロセスで使用される割り当て済みメモリの割合をモニターします。 • メモリ使用率 Snort：Snort プロセスによって使用される割り当て済みメモリの割合をモニターします。

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
ヘルスモニターの機能拡張。	6.7	いずれか	ヘルスモニターには、次の機能拡張が追加されています。 • [正常性ステータス（Health Status）] サマリーページでは、Firepower Management Center と Firewall Management Center が管理するすべてのデバイスの正常性を一目で確認できます。 • [Monitoring] ナビゲーションペインでは、デバイス階層を移動できます。 • 管理対象デバイスは、個別に一覧表示されるか、該当する場合は地理位置情報、高可用性、またはクラスタステータスに基づいてグループ化されます。 • ナビゲーションペインから個々のデバイスのヘルスモニターを表示できます。 • 相互に関連するメトリックを相互に関連付けるカスタムダッシュボード。CPU や Snort などの事前定義された相関グループから選択します。または、使用可能なメトリックグループから独自の変数セットを作成して、カスタム相関ダッシュボードを作成します。
[デバイスでの脅威データの更新（Threat Data Updates on Devices）] モジュールへの機能の移動。	6.7	いずれか	[ローカルマルウェア分析（Local Malware Analysis）] モジュールは使用されなくなりました。この情報については、代わりに [デバイスでの脅威データの更新（Threat Data Updates on Devices）] モジュールを参照してください。 以前は [セキュリティインテリジェンス（Security Intelligence）] モジュールと [URLフィルタリング（URL Filtering）] モジュールによって提供されていた一部の情報が、[デバイスでの脅威データの更新（Threat Data Updates on Devices）] モジュールによって提供されるようになりました。
新しい正常性モジュール：[構成メモリ割り当て（Configuration Memory Allocation）]。	7.0 6.6.3	任意（Any）	バージョン 6.6.3 では、デバイスのメモリ管理が改善され、新しい正常性モジュールである [構成メモリ割り当て（Configuration Memory Allocation）] が導入されています。 このモジュールは、展開された設定のサイズに基づき、デバイスのメモリが不足するリスクがある場合にアラートを出します。アラートには、設定に必要なメモリ量と、使用可能なメモリ量を超過した量が示されます。アラートが出た場合は、設定を再評価してください。ほとんどの場合、アクセス制御ルールまたは侵入ポリシーの数または複雑さを軽減できます。

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
URLフィルタリングモニターの改善。	6.5	任意（Any）	[URLフィルタリングモニター（URL Filtering Monitor）] モジュールは、Firewall Management Center が Cisco Cloud への登録に失敗した場合にアラートを出すようになりました。
URLフィルタリングモニターの改善。	6.4	任意（Any）	URL フィルタリング モニター アラートの時間しきい値を設定できるようになりました。
新しい正常性モジュール：デバイス上での脅威データの更新。	6.3	任意（Any）	新しいモジュールの [デバイス上での脅威データの更新（Threat Data Updates on Devices）] を追加しました。 このモジュールは、デバイスが脅威の検出に使用する特定のインテリジェンス データと設定が指定した時間内にデバイス上で更新されなかった場合にアラートを発行します。

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。