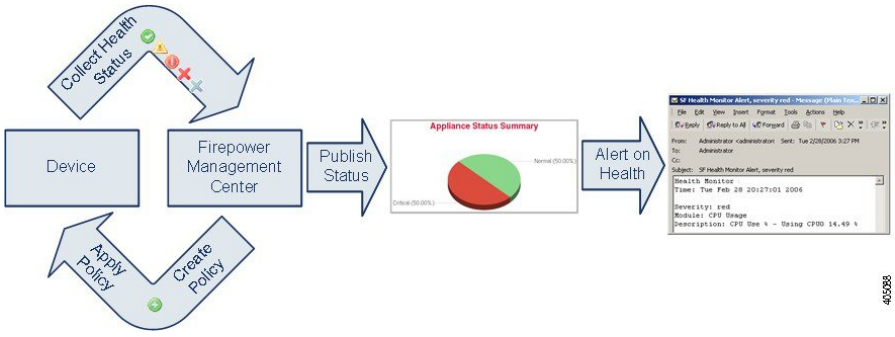
ヘルス モニタリング

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 モニタリングについて

Firepower Management Center のヘルス モニタでは、さまざまなヘルス インジケータを追跡して Firepower 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。ヘルス モニタを使用して、Firepower システム展開全体の重要な機能のステータスを確認できます。



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。ヘルス 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。アプライアンスをブラックリストに登録することによって、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。

正常性ポリシー内のテストは設定された時間間隔で自動的に実行されます。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、Firepower 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、Firepower Management Center 上で実行され Firepower Management Center の管理対象デバイスのステータスを報告します。ヘルス モジュールによっては、そのモジュールが設定されている正常性ポリシーをデバイスに適用しない限り管理対象デバイスのステータスを報告しないものもあります。

ヘルス モニタを使用してシステム全体、特定のアプライアンス、または特定のドメイン（マルチドメイン展開の場合）に関するヘルス ステータス情報にアクセスできます。[ヘルス モニタ（Health Monitor）] ページの円グラフとステータス テーブルには、Firepower 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の視覚的なサマリが示されます。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が原因で障害が発生することは絶対ないことを確認する必要がある場合は、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その電子メールアラートをトリガーとして使用するヘルス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。

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。

ヘルス モニタリングは管理活動であるため、管理者ユーザ ロール特権を持っているユーザのみがシステム ヘルス データにアクセスできます。

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。

表 *1*: ヘルス モジュール

モジュール	[アプライアンス（**Appliances**）]	説明
AMP for Endpoint のステータス	FMC	このモジュールは、Firepower 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、AMP for Endpoints 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 （ネットワーク向け AMP ステータス）	FMC	このモジュールは、以下の場合にアラートを出します。 • Firepower Management Center が AMP クラウド（パブリックまたはプライベート）、Cisco Threat Grid パブリック クラウド、またはオンプレミス 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 Cisco Threat Grid クラウドまたは Cisco Threat Grid オンプレミス 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。 Firepower Management Center のインターネット接続が切断された場合、AMP for Firepower ステータス 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	任意（Any）	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。
自動アプリケーション バイパス ステータス	7000 & 8000 シリーズ	このモジュールは、アプライアンスがバイパスしきい値で設定された秒数以内に応答しなかったためにバイパスされたかどうかを確認し、バイパスが発生した場合にアラートを出します。
バックログのステータス	FMC	このモジュールは、デバイスから FMC 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表示します。 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。

モジュール	[アプライアンス（Appliances）]	説明
クラシック ライセンス モニタ	FMC	このモジュールは、制御、保護、URL フィルタリング、マルウェア、および VPN 用の十分なクラシック ライセンスが残っているかどうかを確認します。また、スタック内のデバイスに適合しないライセンス セットが含まれている場合にアラートを出します。モジュールに自動的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。このモジュールの設定は変更できません。
CPU 使用率	任意（Any）	このモジュールは、アプライアンス上の CPU 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。
カード リセット	任意（Any）	このモジュールは、リセット時に、ハードウェア障害原因で再起動されたネットワーク カードをチェックし、アラートを出します。
クラスタのステータス	脅威防御	このモジュールは、デバイス クラスタのステータスをモニタします。このモジュールは、以下の場合にアラートを出します。 • クラスタに新しいプライマリ ユニットが選択される。 • 新しいセカンダリ ユニットがクラスタに参加する。 • プライマリまたはセカンダリ ユニットがクラスタから離脱する。
ディスク ステータス	任意（Any）	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。
ディスク使用量	任意（Any）	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。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。

モジュール	[アプライアンス（Appliances）]	説明
ホスト制限	FMC	このモジュールは、Firepower Management Center がモニタ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、Firepower システムのホスト制限を参照してください。
ハードウェア アラーム	7000 & 8000 シリーズ Threat Defense（物理）	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。また、ハードウェア関連デーモンのステータスとハイ アベイラビリティ展開の 7000 および 8000 シリーズ デバイスのステータスについてレポートします。
HA ステータス	FMC	このモジュールは、Firepower Management Center ハイ アベイラビリティ ステータスについて、モニタし、アラートを出します。Firepower Management Center のハイ アベイラビリティを確立していない場合、HA ステータスは、「HA でない（Not in HA）」になります。 このモジュールは、ペアリングされているかどうかに関わらず、管理対象デバイスのハイ アベイラビリティ ステータスについてはモニタしたり、アラートを出したりしません。管理対象デバイスの HA ステータスは常に「HA でない（Not in HA）」になります。**[Devices]** > **[Device Management]** の [デバイス管理（Device Management）] ページを使用して、ハイ アベイラビリティ ペアのデバイスをモニタします。
ヘルス モニタ プロセス	任意（Any）	このモジュールは、ヘルス モニタ自体のステータスを監視し、Firepower Management Center で受信された最後のステータス イベント以降の分数が警告制限または重大制限を超えた場合にアラートを出します。
インライン リンク不一致アラーム	ASA FirePOWER を除くすべての管理対象デバイス	このモジュールは、インライン セットに関連付けられたポートを監視し、インライン ペアの 2 つのインターフェイスが別々の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	[アプライアンス（Appliances）]	説明
侵入およびファイル イベント レート	すべての管理対象デバイス	このモジュールは、1 秒あたりの侵入イベント数をこのモジュールに設定された制限と比較し、制限を超えた場合にアラートを出します。侵入およびファイル イベント レートが 0 の場合は、侵入プロセスがダウンしているか、管理対象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。イベントがデバイスから送られているかどうかをチェックするには、**[Analysis]** > **[Intrusions]** > **[Events]** の順に選択します。 一般に、ネットワーク セグメントのイベント レートは平均で 1 秒あたり 20 イベントです。この平均レートのネットワーク セグメントでは、[1 秒あたりのイベント（重大）（Events per second (Critical)）] を 50 に設定し、[1 秒あたりのイベント（警告）（Events per second (Warning)）] を 30 に設定する必要があります。システムの制限を決定するには、デバイスの [統計情報（Statistics）] ページ（**[System]** > **[Monitoring]** > **[Statistics]**）で [イベント/秒（Events/Sec）] 値を探してから、次の式を使用して制限を計算します。 • 1 秒あたりのイベント（重大）= イベント/秒 * 2.5 • イベント数/秒（警告）（Events per second (Warning)）= イベント数/秒（Events/Sec）* 1.5 両方の制限に設定可能な最大イベント数は 999 であり、重大制限は警告制限より大きくする必要があります。
インターフェイス ステータス	任意（Any）	このモジュールは、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。 ASA FirePOWER の場合、DataPlaneInterfacex というラベルの付いたインターフェイス（ここで、xは数値）は、内部インターフェイス（ユーザ定義ではない）で、システム内部のパケット フローに関与します。

モジュール	[アプライアンス（Appliances）]	説明
リンク ステート伝達	NGIPSv、ASA FirePOWER、Firepower 9300、Firepower 4100 シリーズ、Firepower 2100 シリーズ を除き任意	このモジュールは、ペア化されたインラインセット内のリンクで障害が発生した時点を特定して、リンク ステート伝達モードをトリガーとして使用します。 リンク ステートがペアに伝達した場合は、そのモジュールのステータス分類が [重大（Critical）] に変更され、状態が次のように表示されます。 `Module Link State Propagation: ethx_ethy is Triggered` ここで、`x` と `y` はペア化されたインターフェイス番号です。
ローカルマルウェア分析	任意（Any）	このモジュールは、6.3 よりも前のバージョンを実行中のデバイスがローカル マルウェア分析用に設定され、AMP クラウドからローカル マルウェア分析エンジンの署名の更新をダウンロードできなかった場合、アラートを出します。 6.3 以降のバージョンを実行しているデバイスの場合は、[デバイスの脅威データの更新（Threat Data Updates on Devices）] モジュールを確認します。
メモリ使用率	任意（Any）	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 未満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。 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。FirePOWER サービス ソフトウェア を含む一部のよりローエンドの ASA デバイスでは、デバイスのメモリ割り当てが最大限に使用されているため、断続的なメモリ使用率の警告が生成されることがあります。

モジュール	[アプライアンス（Appliances）]	説明
プラットフォームの障害	Firepower 2100	Firepower 2100 デバイスでは、障害は Firepower Management Center によって管理される変更可能なオブジェクトです。各障害は、Firepower 2100 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。障害のライフサイクルの間に、障害の状態または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 2100 FXOS Faults and Error Messages Guide*』を参照してください。
電源モジュール	物理 FMC 7000 & 8000 シリーズ	このモジュールは、デバイスの電源が交換が必要かどうかを確認し、電源ステータスに基づいてアラートを出します。 （注） 8000 シリーズ管理対象デバイスで電源障害が発生した場合、アラートを生成するために最大 20 分かかることがあります。
Process Status	任意（Any）	このモジュールは、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かを確認します。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。
検出の再設定	すべての管理対象デバイス	このモジュールは、デバイスの再設定が失敗した場合、アラートを出します。
RRD サーバ プロセス	FMC	このモジュールは、時系列データを格納するラウンド ロビン サーバが正常に機能しているかどうかを確認します。このモジュールは、RRD サーバ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。また、RRD サーバの再起動を伴う連続更新回数がモジュール設定で指定された数値に達した場合に [重大（Critical）] または [警告（Warning）] ステータスに遷移します。

モジュール	[アプライアンス（Appliances）]	説明
セキュリティ インテリジェンス（Security Intelligence）	FMC および一部の管理対象デバイス	このモジュールは、セキュリティ インテリジェンスが使用中で、次の場合にアラートを出します。 • Firepower 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、または認識可能な IP アドレスが含まれていない。 • 6.3 よりも前のリリースを実行中の管理対象デバイスで、Firepower Management Center からの更新済みセキュリティ インテリジェンス データを受信する際に問題が発生しました 。 • 6.3 よりも前のリリースを実行中の管理対象デバイスが、メモリの問題により、Firepower Management Center から提供されたすべてのセキュリティ インテリジェンス データをロードできません。メモリ使用のトラブルシューティング を参照してください。 • 6.3 以降のバージョンを実行している管理対象デバイスの場合は、[デバイスの脅威データの更新（Threat Data Updates on Devices）] モジュールを確認します。
スマート ライセンス モニタ	FMC	このモジュールは、以下の場合にアラートを出します。 • Smart Licensing Agent 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	[アプライアンス（Appliances）]	説明
デバイスでの脅威データの更新	リリース 6.3 以降を実行中の FMC およびデバイス （6.3 よりも前のバージョンを実行中のデバイスの場合、セキュリティ インテリジェンス、URL フィルタリング、およびローカルマルウェア分析ヘルスモジュールに関する次の表を参照してください）。	

モジュール	[アプライアンス（Appliances）]	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、Firepower 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 ホワイト リストとブラック 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 ホワイト リストとブラック 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 ホワイト リストとブラック 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） • [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 の期限切れに関連した脅威の構成時の設定（[システム（System）] > [統合（Integration）] **[Cisco CSI]**ページでの [キャッシュされたURLの期限切れ（Cached URLs Expire）] 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されません。） （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。 FMC 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、Firepower Management Center がデバイス

モジュール	[アプライアンス（Appliances）]	説明
		に到達できることを確認します。 URL カテゴリおよびレピュテーション データ タイプの障害が表示される低メモリ デバイスについては、メモリ使用のトラブルシューティング を参照してください。
時系列データ モニタ	FMC	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。
時刻同期ステータス	任意（Any）	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。
URL フィルタリング モニタ	FMCについて 6.3 以降のバージョンを実行しているデバイスの場合は、[デバイスの脅威データの更新（Threat Data Updates on Devices）] モジュールも確認します。	このモジュールは、Firepower Management Center が次のことに失敗した場合にアラートを出します。 • Cisco Collective Security Intelligence（CSI）との通信または CSI からの URL 脅威インテリジェンス データの更新の取得。 • （6.3 よりも前のバージョンを実行中のデバイスの場合）URL 脅威データの管理対象デバイスへのプッシュ （6.3 以降のバージョンを実行しているデバイスの場合は、[デバイスの脅威データの更新（Threat Data Updates on Devices）] モジュールで、この問題のためのアラートを設定してください）。
ユーザ エージェント ステータス モニタ	FMC	このモジュールは、Firepower Management Center に接続されたユーザ エージェントでハートビートが検出されない場合にアラートを出します。
VPN ステータス	FMC	このモジュールは、Firepower システム デバイス間の 1 つ以上の VPN トンネルがダウンしているときにアラートを出します。 このモジュールは、以下を追跡します。 • 7000 & 8000 シリーズ デバイスの VPN） • Firepower Threat Defense のサイト間 VPN • Firepower Threat Defense のリモート アクセス VPN

ヘルス モニタリングの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Maint

手順

ステップ 1 ヘルス モジュール （2 ページ）で説明されているように、モニタするヘルス 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 （14 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 アラートの作成 （22 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されたヘルス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。

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。マルチドメイン展開では、先祖ドメインの管理者が子孫ドメインのデバイスに正常性ポリシーを適用できます。子孫ドメインではそのポリシーを使用するか、またはカスタマイズされたローカル ポリシーと置き換えることができます。

デフォルトの正常性ポリシー

Firepower Management Center のヘルス モニタでは、アプライアンスのヘルス モニタリングを迅速に実行できるように、デフォルトの正常性ポリシーが提供されます。デフォルト正常性ポリシーでは、実行中のプラットフォーム上で使用可能なヘルス モジュールのほとんどが自動的に有効になります。デフォルト正常性ポリシーは、自動的にFirepower Management Centerに適用されます。また、Firepower Management Center にデバイスを追加すると、デフォルトの正常性ポリシーが管理対象デバイスに適用されます。デフォルト正常性ポリシーを編集することはできませんが、コピーしてその設定に基づくカスタム ポリシーを作成することができます。

正常性ポリシーの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Maint

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。必要に応じて、ポリシー内のモジュールを有効または無効にし、各モジュールのアラート基準を変更できます。

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。 先祖ドメインの管理者は、子孫ドメインのデバイスに正常性ポリシーを適用でき、子孫ドメインはこれを使用するか、またはカスタマイズしたローカル ポリシーに置き換えることができます。

手順

ステップ 1 **[System]** > **[Health]** > **[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 [コピー ポリシー（Copy 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 4 ポリシーの名前を入力します。

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）] を選択して、ポリシー情報を保存します。

ステップ 7 使用するモジュールを選択します。

ステップ 8 [有効（Enabled）] オプションに対して [オン（On）] を選択して、ヘルス ステータス テストのモジュールの使用を有効化します。

ステップ 9 該当する場合は、[重大（Critical）] および [警告（Warning）] 基準を設定します。

ステップ 10 モジュールの追加設定を行います。各モジュールで手順 7 ～ 10 を繰り返します。

ステップ 11 次の 3 つのオプションがあります。

- このモジュールに対する変更を保存して、[正常性ポリシー（Health Policy）] ページに戻るには、[ポリシーを保存して終了（Save Policy and Exit）] をクリックします。
- このモジュールの設定を保存せずに、[正常性ポリシー（Health Policy）] ページに戻るには、[キャンセル（Cancel）] をクリックします。
- このモジュールに対する変更を一時的に保存して、変更する他のモジュールの設定に切り替えるには、ページの左側にあるリストから他のモジュールを選択します。設定が終わって [ポリシーを保存して終了（Save Policy and Exit）] をクリックすると、加えたすべての変更が保存されます。[キャンセル（Cancel）] をクリックすると、すべての変更が破棄されます。

次のタスク

- 正常性ポリシーの適用 （15 ページ）の説明に従って、各アプライアンスに正常性ポリシーを適用します。これにより変更が適用され、影響を受けるすべてのポリシーのポリシー ステータスが更新されます。

正常性ポリシーの適用

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Maint

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Firepower 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。

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。

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。先祖ドメインの管理者は、子孫ドメインのデバイスに正常性ポリシーを適用でき、子孫ドメインはこれを使用するか、またはカスタマイズしたローカル ポリシーに置き換えることができます。

手順

ステップ 1 **[System]** > **[Health]** > **[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適用アイコン（）をクリックします。

ヒント [正常性ポリシー（Health Policy）] 列の横にあるステータス アイコン（）は、アプライアンスの現在のヘルス ステータスを示します。

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。

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た直後に開始されます。

正常性ポリシーの編集

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Maint

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。 先祖ドメインの管理者は、子孫ドメインのデバイスに正常性ポリシーを適用でき、子孫ドメインはこれを使用するか、またはカスタマイズしたローカル ポリシーに置き換えることができます。

手順

ステップ 1 **[System]** > **[Health]** > **[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アイコン（）をクリックします。

ステップ 3 [ポリシー名（Policy Name）] フィールドまたは [ポリシーの説明（Policy Description）] フィールドを必要に応じて編集します。

ステップ 4 変更するヘルス モジュールをクリックします。

ステップ 5 ヘルス モジュール （2 ページ）の説明に従って、設定を変更します。

ステップ 6 次の 3 つのオプションがあります。

- このモジュールに対する変更を保存して、[正常性ポリシー（Health Policy）] ページに戻るには、[ポリシーを保存して終了（Save Policy and Exit）] をクリックします。
- このモジュールの設定を保存せずに、[正常性ポリシー（Health Policy）] ページに戻るには、[キャンセル（Cancel）] をクリックします。
- このモジュールに対する変更を一時的に保存して、変更する他のモジュールの設定に切り替えるには、ページの左側にあるリストから他のモジュールを選択します。設定が終わって [ポリシーを保存して終了（Save Policy and Exit）] をクリックすると、加えたすべての変更が保存されます。[キャンセル（Cancel）] をクリックすると、すべての変更が破棄されます。

次のタスク

- 正常性ポリシーの適用 （15 ページ）の説明に従って、正常性ポリシーを再適用します。これにより変更が適用され、影響を受けるすべてのポリシーのポリシー ステータスが更新されます。

正常性ポリシーの削除

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Maint

不要になった正常性ポリシーを削除できます。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。

マルチドメイン導入では、現在のドメインで作成された正常性ポリシーのみを削除できます。

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 **[System]** > **[Health]** > **[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アイコン（）をクリックします。
削除が成功したかどうかを示すメッセージが表示されます。

ヘルス モニタ ブラックリスト

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 Firepower 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 ブラックリスト機能を使用して、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、Firepower 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 モニタのヘルス ステータスには影響しません。ブラック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、ブラックリストに登録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、ブラックリスト設定ページに移動して、アプライアンスをブラックリストに追加します。設定が有効になると、システムは全体のヘルス ステータスを計算するときにブラックリストに登録されているアプライアンスを含めません。[ヘルス モニタ 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。

アプライアンス上の個別のヘルス モニタリング モジュールをブラックリストに登録する方が実用的な場合があります。たとえば、Firepower 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 メッセージをブラックリストに登録できます。

メインの [ヘルス モニタ（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、ブラックリストに登録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。

ブラックリストに登録されたアプライアンスまたは部分的にブラックリストに登録されたアプライアンスのビューを展開すると、ブラックリスト アイコン（）と注記が表示されます。

（注） Firepower Management Center では、ヘルス モニタのブラックリスト設定はローカル コンフィギュレーション設定です。そのため、Firepower Management Center 上でデバイスをブラックリストに登録してから削除しても、後で再登録すれば、ブラックリスト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ブラックリストに登録されたままです。

マルチドメイン導入では、先祖ドメインの管理者が子孫ドメインのアプライアンスやヘルス モジュールをブラックリストに登録できます。ただし、子孫ドメインの管理者は、先祖のコンフィギュレーションをオーバーライドして、自身のドメインのデバイスのブラックリストをクリアすることができます。

アプライアンスのブラックリスト登録

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Maint

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、ブラックリストに登録できます。

ブラックリスト設定が有効になると、[正常性モニタアプライアンスモジュールの概要（Health Monitor Appliance Module Summary）] と [デバイス管理（Device Management）] ページでアプライアンスが [無効（Disabled）] として表示されます。アプライアンスのヘルス イベントのステータスは [無効（Disabled）] です。

個別のアプライアンスのイベントとヘルス ステータスを [無効（Disabled）] に設定する必要がある場合、アプライアンスをブラックリストに登録できます。ブラックリスト設定が有効になると、アプライアンスが [正常性モニタ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、アプライアンスのヘルス イベントのステータスが [無効（Disabled）] になります。

マルチドメイン展開では、アプライアンスを先祖ドメインのブラックリストに登録すると、子孫ドメインもすべてブラックリストに登録されたことになります。子孫ドメインは、この設定の継承をオーバーライドし、ブラックリスト指定を解除できます。Firepower Management Center はグローバル レベルでのみブラックリスト指定できます。

手順

ステップ 1 **[System]** > **[Health]** > **[Blacklist]**を選択します。

ステップ 2 アプライアンス グループ、モデル、またはポリシーでリストをソートするには、右側にあるドロップダウンリストを使用します。

ヒント [正常性ポリシー（Health Policy）] 列の横にあるステータス アイコン（）は、アプライアンスの現在のヘルス ステータスを示します。[システムポリシー（System Policy）] 列の横にあるステータス アイコン（）は、Firepower Management Center とデバイス間の通信ステータスを示します。

ステップ 3 次の 2 つの選択肢があります。

- グループ、モデル、またはポリシー カテゴリ内のすべてのアプライアンスをブラックリストに登録するには、カテゴリのチェックボックスをオンにしてから、[選択したデバイスをブラックリストに登録（Blacklist Selected Devices）] をクリックします。

- グループ、モデル、またはポリシー カテゴリ内のすべてのアプライアンスをブラックリストから除外するには、カテゴリのチェックボックスをオンにしてから、[選択したデバイスのブラックリスト指定を解除（Clear Blacklist on Selected Devices）] をクリックします。

正常性ポリシー モジュールのブラックリスト登録

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Maint

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ブラックリストに登録できます。この操作により、モジュールからのイベントによってアプライアンスのステータスが Warning または Critical に変更されないようにすることができます。

ブラックリスト設定が有効になると、アプライアンスが [ブラックリスト（Blacklist）] ページと [アプライアンス正常性モニタモジュールステータスの概要（Appliance Health Monitor Module Status Summary）] で [部分的なブラックリスト指定（Partially Blacklisted）] または [すべてのモジュールがブラックリスト指定（All Modules Blacklisted）] として表示されますが、メインの [アプライアンスのステータスの概要（Appliance Status Summary）] ページでは展開されたビューにだけ表示されます。

ヒント　個別にブラックリストに登録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、必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。

マルチドメイン展開では、先祖ドメインの管理者は子孫ドメインの正常性モジュールをブラックリストに登録できます。しかし、子孫ドメインの管理者は、この先祖の設定をオーバーライドし、ドメインに適用されるポリシーのブラックリスト指定を解除できます。Firepower Management Center 正常性モジュールはグローバル レベルでのみブラックリスト指定できます。

手順

ステップ 1　**[System]** > **[Health]** > **[Blacklist]** を選択します。

ステップ 2　変更するアプライアンスの横にある編集アイコン（ ）をクリックします。

ステップ 3　ブラックリスト指定する正常性ポリシーモジュールの横にあるチェックボックスをオンにします。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 （2 ページ） を参照してください。

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

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、またはシステム ログ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。

マルチドメイン展開では、現在のドメインで作成されたヘルス モニタのアラートのみを表示、および変更できます。

ヘルス モニタ 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 *2:* アラートの重大度

重大度	説明
クリティカル（Critical）	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 アラートの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin

ヘルス モニタ アラートを作成するときに、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。

マルチドメイン導入では、現在のドメインで作成されたヘルス モニタ アラートのみを表示および変更できます。

始める前に

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

手順

ステップ 1 **[System]** > **[Health]** > **[Monitor Alerts]**を選択します。

ステップ 2 [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 3 [重大度（Severity）] 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 4 [モジュール（Module）] 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 5 [アラート（Alert）] 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。

ステップ 6 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 7 [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

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin

既存のヘルス モニタ アラートを編集して、ヘルス モニタ 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。

マルチドメイン導入では、現在のドメインで作成されたヘルス モニタ アラートのみを表示および変更できます。

手順

ステップ 1 **[System]** > **[Health]** > **[Monitor Alerts]**を選択します。

ステップ 2 [アクティブ ヘルス アラート（Active Health Alerts）] リストから、変更するアラートを選択します。

ステップ 3 [ロード（Load）] をクリックして、選択したアラートの構成済みの設定をロードします。

ステップ 4 必要に応じて設定を変更します。

ステップ 5 [保存（Save）] をクリックして、変更したヘルス アラートを保存します。
アラート設定が正常に保存されたかどうかを示すメッセージが表示されます。

ヘルス モニタ アラートの削除

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin

マルチドメイン導入では、現在のドメインで作成されたヘルス モニタ アラートのみを表示および変更できます。

手順

ステップ 1 **[System]** > **[Health]** > **[Monitor Alerts]**を選択します。

ステップ 2 削除するアクティブなヘルス アラートを選択してから、[削除（Delete）] をクリックします。

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。Firepower Management Center アラート応答を参照してください。

ヘルス モニタの使用

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Maint/Any Security Analyst

ヘルス モニタには、Firepower 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、Firepower Management Center 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。

- ステータス テーブル：この Firepower Management Center の管理対象アプライアンスの台数が全体のヘルス ステータス別に表示されます。
- 円グラフ：それぞれのヘルス ステータス カテゴリにおけるアプライアンスの現在のパーセンテージを示します。
- アプライアンス リスト：管理対象デバイスのヘルス状態の詳細が表示されます。

マルチドメイン展開では、先祖ドメインのヘルス モニタに、すべての子孫ドメインからのデータが表示されます。子孫ドメインには、現在のドメインからのデータのみが表示されます。

手順

ステップ 1 **[System]** > **[Health]** > **[Monitor]**を選択します。

ステップ 2 テーブルの [ステータス（Status）] カラム内の該当するステータスまたは円グラフの該当する部分を選択して、そのステータスを持つアプライアンスをリストします。

ヒント ステータス レベルに関する行内の矢印が下向きの場合は、そのステータスのアプライアンス リストが下側のテーブルに表示されます。矢印が右向きの場合、アプライアンス リストは非表示です。

ステップ 3 次の選択肢があります。

- アプライアンスのヘルス モニタを表示します（アプライアンス ヘルス モニタの表示 （26 ページ）を参照）。
- ヘルス ポリシーを作成します（正常性ポリシーの作成 （14 ページ）を参照）。

- ヘルス モニタ アラートを作成します（ヘルス モニタ アラートの作成 （22 ページ）を参照）。

ヘルス モニタ 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、重大度別に次の表に示します。

表 *3*: 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）		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（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		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。
標準		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。

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
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		青	アプライアンスが無効またはブラックリストに登録されている、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。

アプライアンス ヘルス モニタの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Maint/Any Security Analyst

アプライアンス ヘルス モニタは、アプライアンスのヘルス ステータスの詳細ビューを提供します。

マルチドメイン展開では、子孫ドメインのアプライアンスのヘルス ステータスを表示できます。

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、Web インターフェイスでの内部ユーザの追加およびセッション 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　**[System]** > **[Health]** > **[Monitor]** を選択します。

ステップ 2 アプライアンス リストを展開します。特定のステータスを持つアプライアンスを表示するには、そのステータス行内の矢印をクリックします。または、[アプライアンス ステータスの概要（Appliance Status Summary）] グラフで、表示するアプライアンス ステータス カテゴリの色をクリックします。

ヒント ステータス レベルに関する行内の矢印が下向きの場合は、そのステータスのアプライアンス リストが下側のテーブルに表示されます。矢印が右向きの場合、アプライアンス リストは非表示です。

ステップ 3 アプライアンス リストの [アプライアンス（Appliance）] 列で、詳細を表示するアプライアンスの名前をクリックします。

ヒント [モジュール ステータスの概要（Module Status Summary）] グラフで、そのステータス カテゴリの [アラート詳細（Alert Details）] の表示を切り替えるには、イベント ステータス カテゴリの色をクリックします。

次のタスク

- アプライアンスのすべてのヘルス モジュールを実行する場合、次を参照してください。 アプライアンスのすべてのモジュールの実行 （27 ページ）
- アプライアンスの特定のヘルス モジュールを実行する場合、次を参照してください。 特定のヘルス モジュールの実行 （28 ページ）
- アプライアンスのヘルス モジュール アラート グラフを生成する場合、次を参照してください。 ヘルス モジュール アラート グラフの生成 （29 ページ）
- アプライアンスのトラブルシューティング ファイルを生成する場合、次を参照してください。 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
- アプライアンスの高度なトラブルシューティング ファイルを生成する場合、次を参照してください。 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
- Firepower Management Center Web インターフェイスから Firepower Threat Defense CLI コマンドを実行する場合はWeb インターフェイスからの FTD CLI の使用を参照してください。

アプライアンスのすべてのモジュールの実行

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Maint/Any Security Analyst

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。

マルチドメイン展開では、現在のドメイン内のアプライアンスと、子孫ドメイン内のアプライアンスに対してヘルス モジュール テストを実行できます。

手順

ステップ 1 アプライアンスのヘルス モニタを表示します。アプライアンス ヘルス モニタの表示（26 ページ）を参照してください。

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 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

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Maint/Any Security Analyst

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。

マルチドメイン展開では、現在のドメイン内のアプライアンスと、子孫ドメイン内のアプライアンスに対してヘルス モジュール テストを実行できます。

手順

ステップ 1 アプライアンスのヘルス モニタを表示します。アプライアンス ヘルス モニタの表示（26 ページ）を参照してください。

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 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

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Maint/Any Security Analyst

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 モニタを表示します（アプライアンス ヘルス モニタの表示（26 ページ）を参照）。

ステップ 2 [ヘルス モニタ 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。

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、Firepower 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

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Maint/Any Security Analyst

[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。

Firepower Management Center 上の [ヘルス モニタ（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。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

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

[System] > **[Health]** > **[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。

モジュールとアプライアンス別のヘルス イベントの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Maint/Any Security Analyst

手順

ステップ 1 アプライアンスのヘルス モニタを表示します（アプライアンス ヘルス モニタの表示（26 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

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Maint/Any Security Analyst

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

ステップ 1 **[System]** > **[Health]** > **[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）] カラムのステータス アイコンをクリックします。

7000 および 8000 シリーズ デバイスのハードウェア アラートの詳細

（注） 8350 ハードウェア プラットフォームには 6 つのファンがあり、FAN2 ～ FAN7 と表示されています。これは想定されている動作です。8350 プラットフォームで FAN1 またはファンの番号付けに関するハードウェア アラートを受け取った場合は、アラートを無視できます。

表 *4 : 7000* および *8000* シリーズ デバイスの監視対象条件

監視対象条件	黄色または赤色エラー状態の原因
デバイスの高可用性ステータス	高可用性ペアの 7000 または 8000 シリーズ デバイスが相互に通信していない（ケーブル配線の問題などで）場合は、ハードウェアアラーム モジュールが赤色に変化します。
`ftwo` デーモン ステータス	`ftwo` デーモンがダウンすると、ハードウェア アラーム モジュールのヘルス ステータスが赤色に変化し、メッセージ詳細にデーモンへの参照が追加されます。
検出された NFE カード	システム上で検出された NFE カードの枚数を示します。この値がアプライアンスの予想NFE カウントと一致しない場合は、ハードウェア アラーム モジュールが赤色に変化します。
NFE ハードウェア ステータス	1 つ以上の NFE カードが通信していない場合は、ハードウェア アラーム モジュールが赤色に変化し、該当するカードがメッセージ詳細に表示されます。
NFE ハートビート	システムが NFE ハートビートを検出しなかった場合は、ハードウェア アラーム モジュールが赤色に変化し、メッセージ詳細に関連カードへの参照が追加されます。
NFE 内部リンク ステータス	NMSB カードと NFE カード間のリンクがダウンした場合は、ハードウェア アラーム モジュールが赤色に変化し、メッセージ詳細に関連ポートへの参照が追加されます。
NFE メッセージ デーモン	NFE メッセージ デーモンがダウンすると、ハードウェア アラーム モジュールのヘルス ステータスが赤色に変化し、メッセージ詳細にデーモンへの参照（および該当する場合はNFE カード番号）が追加されます。

監視対象条件	黄色または赤色エラー状態の原因
NFE 温度	NFE 温度が 97 ℃を超えると、ハードウェア アラーム モジュールのヘルス ステータスが黄色に変化し、メッセージ詳細に NFE 温度への参照（および該当する場合は NFE カード番号）が追加されます。 NFE 温度が 102 ℃を超えると、ハードウェア アラーム モジュールのヘルス ステータスが赤色に変化し、メッセージ詳細に NFE 温度への参照（および該当する場合は NFE カード番号）が追加されます。
NFE 温度ステータス	特定の NFE カードの現在の温度ステータスを示します。OK の場合ハードウェア アラーム モジュールは緑色を、警告の場合は黄色を、クリティカルの場合は赤色（および該当する場合は NFE カード番号）を示します。
NFE TCAM デーモン	NFE TCAM デーモンがダウンすると、ハードウェア アラーム モジュールのヘルス ステータスが赤色に変化し、メッセージ詳細にデーモンへの参照（および該当する場合は NFE カード番号）が追加されます。
nfm_ipfragd（ホスト フラグ）デーモン	nfm_ipfragd デーモンがダウンすると、ハードウェア アラーム モジュールのヘルス ステータスが赤色に変化し、メッセージ詳細にデーモンへの参照（および該当する場合は NFE カード番号）が追加されます。
NFE プラットフォーム デーモン	NFE プラットフォーム デーモンがダウンすると、ハードウェア アラーム モジュールのヘルス ステータスが赤色に変化し、メッセージ詳細にデーモンへの参照（および該当する場合は NFE カード番号）が追加されます。
NMSB コミュニケーション	メディア アセンブリが存在しないか、通信していない場合は、ハードウェア アラーム モジュールのヘルス ステータスが赤色に変化し、メッセージ詳細に NFE 温度への参照（および該当する場合は NFE カード番号）が追加されます。

監視対象条件	黄色または赤色エラー状態の原因
psls デーモン ステータス	psls デーモンがダウンすると、ハードウェア アラーム モジュールのヘルス ステータスが赤色に変化し、メッセージ詳細にデーモンへの参照が追加されます。
Rulesd（ホスト ルール）デーモン	Rulesd デーモンがダウンすると、ハードウェア アラーム モジュールのヘルス ステータスが黄色に変化し、メッセージ詳細にデーモンへの参照（および該当する場合は NFE カード番号）が追加されます。
scmd デーモン ステータス	scmd デーモンがダウンすると、ハードウェア アラーム モジュールのヘルス ステータスが赤色に変化し、メッセージ詳細にデーモンへの参照が追加されます。

[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 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
モジュール名（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。
時刻（Time） （検索専用）	ヘルス イベントのタイムスタンプ。

フィールド	説明
説明	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 [実行不可（Unable to Execute）] というラベルが付けられます。
値	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Firepower Management Centerが生成した場合の値は 80 ～ 100 です。
単位（Units）	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Firepower 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。
ステータス（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）]）。
ドメイン（Domain）	管理対象デバイスによって報告されたヘルス イベントの場合は、ヘルス イベントを報告したデバイスのドメイン。Firepower Management Center によって報告されたヘルス イベントの場合は、`Global`。このフィールドは、マルチドメイン展開の場合にのみ存在します。
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

機能	バージョン（Version）	詳細
新規ヘルス モジュール：デバイス上での脅威データの更新	6.3	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。 新しい画面：**[システム（System）]** > **[正常性（Health）]** > **[ポリシー（Policy）]** に新しい正常性ポリシーを表示 変更後の画面：**[システム（System）]** > **[正常性（Health）]** > **[モニタ（Monitor）]** に新しいモニタ結果を表示 サポートされるプラットフォーム：6.3 以降のバージョンを実行している Firepower Management Center および管理対象デバイス
ヘルス モニタリング	—	バージョン 6.0 よりも前に導入された機能です。 新しい画面：**[システム（System）]** > **[正常性（Health）]** にメニュー オプションを表示 サポートされるプラットフォーム：Firepower Management Center および管理対象デバイス