



ヘルス モニタリングの使用

ヘルス モニタは、Defense Center からアプライアンスの正常性を確認するためのさまざまなテストを提供します。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。システム内のすべてのアプライアンスに共通の正常性ポリシーを作成することも、適用を予定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、デフォルトの正常性ポリシーを使用することもできます。別の Defense Center からエクスポートした正常性ポリシーをインポートすることもできます。

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。オプションで、ヘルス イベントに対応して警告する電子メール、SNMP、または syslog を設定することもできます。

Defense Center では、システム全体または特定のアプライアンスに関するヘルス ステータス情報を表示できます。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。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する他の情報にアクセスしたりできます。

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。

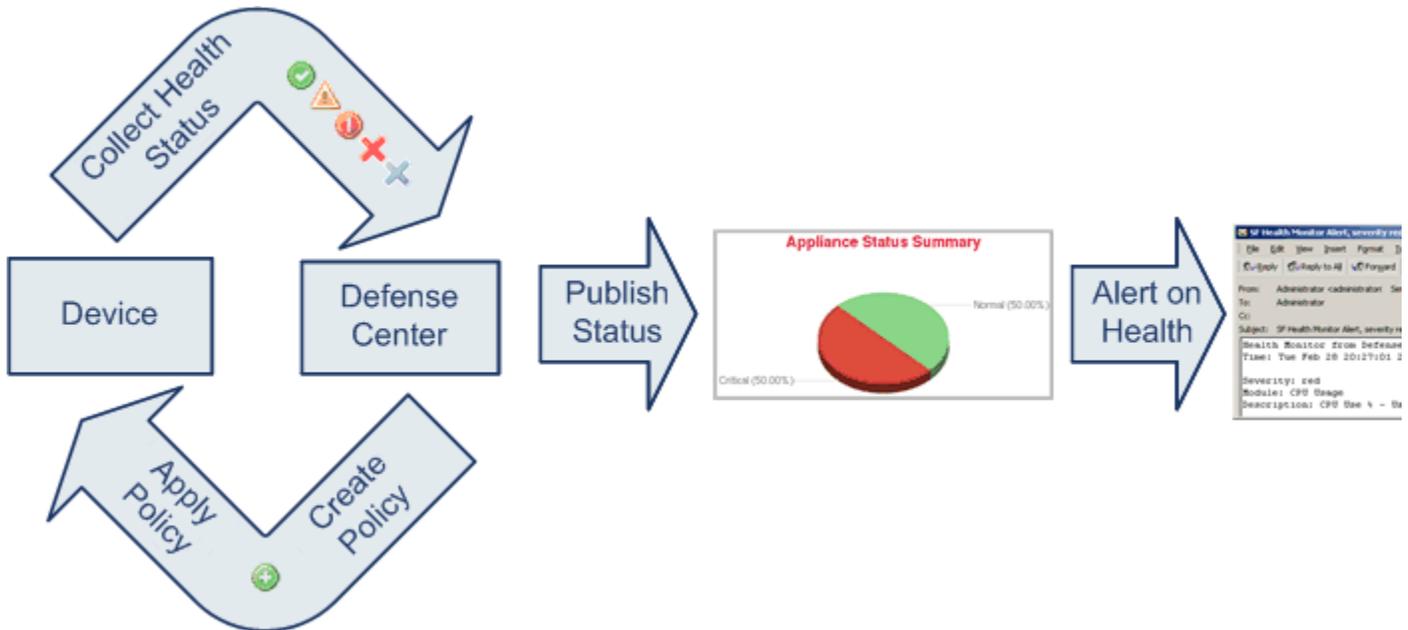
詳細については、次の各項を参照してください。

- [ヘルス モニタリングについて \(68-2 ページ\)](#)
- [正常性ポリシーの設定 \(68-7 ページ\)](#)
- [ヘルス モニタ ブラックリストの使用 \(68-40 ページ\)](#)
- [ヘルス モニタ アラートの設定 \(68-43 ページ\)](#)
- [ヘルス モニタの使用 \(68-46 ページ\)](#)
- [アプライアンス ヘルス モニタの使用 \(68-48 ページ\)](#)
- [ヘルス イベントの操作 \(68-54 ページ\)](#)

ヘルス モニタリングについて

ライセンス:任意(Any)

ヘルス モニタを使用して、FireSIGHT 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。Defense Center を通して管理対象デバイスのそれぞれに正常性ポリシーを適用し、Defense Center で結果のヘルス データを収集することによって、FireSIGHT システム全体の正常性を監視します。[ヘルス モニタ (Health Monitor)] ページ上の円グラフとステータス テーブルは、モニタ対象のアプライアンスのヘルス ステータスを視覚的に表しているため、一目でステータスをチェックでき、必要に応じてステータス詳細にドリルダウンできます。



ヘルス モニタを使用して、システム全体または特定のアプライアンスのヘルス ステータス情報にアクセスできます。[ヘルス モニタ (Health Monitor)] ページには、システム上のすべてのアプライアンスのステータスの概要が表示されます。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。

標準の FireSIGHT システム テーブル ビューでヘルス イベントを表示することもできます。個々のアプライアンスのヘルス モニタから、特定のイベント発生のテーブル ビューを開いたり、そのアプライアンスのすべてのステータス イベントを取得したりできます。特定のヘルス イベントを検索することもできます。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。

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。ユーザ特権の割り当て方法については、[ユーザ特権とオプションの変更 \(61-59 ページ\)](#) を参照してください。



(注)

Defense Center を除いて、FireSIGHT システム デバイスにはデフォルトでヘルス モニタリング ポリシーが適用されません。管理対象デバイスはハードウェア アラーム ヘルス モジュール経由で自動的にハードウェア ステータスを報告します。他のモジュールを使用して管理対象デバイスをモニタする場合は、正常性ポリシーをそのデバイスに適用する必要があります。Cisco が提供するアプライアンス用のデフォルト正常性ポリシーの詳細については、[デフォルト正常性ポリシーについて \(68-8 ページ\)](#) を参照してください。カスタマイズした正常性ポリシーの作成方法については、[正常性ポリシーの作成 \(68-9 ページ\)](#) を参照してください。ポリシーの適用について詳しくは、[正常性ポリシーの適用 \(68-34 ページ\)](#) を参照してください。

正常性ポリシーと、システム ヘルスをテストするために実行可能なヘルス モジュールの詳細については、次のトピックを参照してください。

- [正常性ポリシーについて \(68-3 ページ\)](#)
- [ヘルス モジュールについて \(68-3 ページ\)](#)
- [ヘルス モニタリング設定について \(68-6 ページ\)](#)

正常性ポリシーについて

ライセンス:任意(Any)

正常性ポリシーは、Defense Center がアプライアンスの正常性をチェックするときに使用する基準を定義するためにアプライアンスに適用するヘルス モジュール設定のコレクションです。ヘルス モニタは、FireSIGHT システムのハードウェアとソフトウェアが正しく機能していることを確認するためのさまざまなヘルス インジケータを追跡します。

正常性ポリシーを作成するときに、アプライアンスの正常性を確認するために実行するテストを選択します。また、デフォルト正常性ポリシーをアプライアンスに適用することもできます。

ヘルス モジュールについて

ライセンス:任意(Any)

ヘルス テストとも呼ばれるヘルス モジュールは、正常性ポリシー内で指定された基準に照らしてテストするスクリプトです。使用可能なヘルス モジュールの説明を次の表に示します。

表 68-1 ヘルス モジュール

モジュール	説明
高度なマルウェア防御	このモジュールは、ファイル ポリシー設定に基づいて、ネットワーク トラフィックで検出されたファイルに関するファイル性質情報を取得するため、または動的分析用にファイルを送信するために Defense Center が Collective Security Intelligence クラウドに接続できなかった場合、または、ネットワーク トラフィックで過剰なファイル数が検出された場合に警告します。FireAMP プライベート クラウド経由の接続でも、プライベート クラウドが Cisco のパブリック クラウドに接続できなかった場合にアラートが生成されます。 このモジュールは、高度なマルウェア防御をサポートしていない DC500 を除くすべての Defense Center 上で動作します。
アプライアンス ハートビート	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。

表 68-1 ヘルス モジュール(続き)

モジュール	説明
自動アプリケーションバイパス ステータス	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。
CPU 使用率	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。 このモジュールは、3D9900 デバイスに適用される正常性ポリシーでは使用できません。
カードリセット	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。
ディスクステータス	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。また、ハードディスクと RAID コントローラ(設置されている場合)に障害が発生する恐れがある場合、あるいは、マルウェアストレージパックが設置後に検出されないまたは正規品でない場合にアラートを出します。
ディスク使用量	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、システムがモニタ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。
FireAMP ステータス モニタ	このモジュールは、Defense Center が初期接続の成功後に Cisco クラウドに接続できない場合、または FireAMP ポータルを使用してクラウド接続を登録解除した場合、またはプライベートクラウドがシスコのパブリッククラウドと通信できない場合にアラートを出します。 このモジュールは、Defense Center 上でのみ動作します。
FireSIGHTホスト ライセンス制限	このモジュールは、十分な FireSIGHT ホスト ライセンスが残っ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。 このモジュールは、Defense Center 上でのみ動作します。
ハードウェア アラーム	このモジュールは、シリーズ 3 または 3D9900 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クラスタ化されたアプライアンスのステータスについて報告します。 これらのデバイスについて報告される詳細については、 3D9900 デバイスのハードウェアアラート詳細の解釈 (68-58 ページ) と シリーズ 3 デバイスのハードウェアアラート詳細の解釈 (68-59 ページ) を参照してください。
ヘルス モニタ プロセス	このモジュールは、ヘルス モニタ自体のステータスをモニタし、Defense 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。 このモジュールは、Defense Center 上でのみ動作します。
インラインリンク不一致アラーム	このモジュールは、インラインセッ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。

表 68-1 ヘルス モジュール(続き)

モジュール	説明
侵入イベント レート	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、[分析 (Analysis)] > [侵入 (Intrusions)] > [イベント (Events)] の順に選択します。
インターフェイス ステータス	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。
ライセンス モニタ	このモジュールは、Control、Protection、URL Filtering、Malware、および VPN 用の十分な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。 このモジュールは、Defense Center 上でのみ動作します。
リンク ステート伝達	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特定して、リンク ステート伝達モードをトリガーします。
メモリ使用率	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。
電源	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。 このモジュールは、Defense Center DC1500、DC2000、DC3500、DC4000 上で動作します。 このモジュールは、デバイス 3D3500、3D4500、3D6500、3D9900、および シリーズ 3 上で動作します。
プロセス ステータス	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	このモジュールは、登録された管理対象デバイスでポリシーの適用に失敗した後も検出機能が保持されるかどうかを確認します。ポリシーの適用に失敗して検出機能が動作不能になった場合、モジュールは検出機能が再確立されるまでヘルス アラートを生成します。
RRD サーバプロセス	このモジュールは、時系列データを保存するラウンドロビン データ サーバが正常に動作しているかどうかを確認し、最近の RRD サーバの再起動回数に基づいてアラートを出します。 このモジュールは、Defense Center 上でのみ動作します。
セキュリティ インテリジェンス	このモジュールは、フィード更新、フィード破損、メモリ問題などのセキュリティ インテリジェンス フィルタリングに関するさまざまな状況でアラートを出します。 このモジュールは、セキュリティ インテリジェンス フィルタリングをサポートしていない DC500 以外のすべての Defense Center 上で動作します。

表 68-1 ヘルス モジュール(続き)

モジュール	説明
時系列データ モニタ	このモジュールは、時系列データ(コンプライアンス 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。 このモジュールは、Defense Center 上でのみ動作します。
時刻同期ステータス	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	このモジュールは、通常訪問される URL に関する URL フィルタリング(カテゴリとレピュテーション)データをシステムが取得する Defense Center と Cisco クラウド間の通信を追跡します。Defense Center がクラウドとの通信またはクラウドからの更新の取得に失敗した場合にアラートを出します。 このモジュールは、Defense Center と、URL フィルタリングが有効になっている管理対象デバイス間の通信も追跡します。Defense Center が URL フィルタリング データをそのようなデバイスにプッシュできない場合にアラートを出します。 このモジュールは、URL フィルタリングをサポートしていない DC500 以外のすべての Defense Center 上でのみ動作します。
ユーザ エージェント ステータス モニタ	このモジュールは、Defense 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。 このモジュールは、Defense Center 上でのみ動作します。
VPN ステータス	このモジュールは、VPN 機能が動作していないことをシステムが検出するとアラートを出します。 このモジュールは、Defense Center 上でのみ動作します。

ヘルス モニタリング設定について

ライセンス:任意(Any)

次の手順に示すように、FireSIGHT システム上でヘルス モニタリングをセットアップするためのいくつかのステップがあります。

手順 1 アプライアンス用の正常性ポリシーを作成します。

FireSIGHT 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。

正常性ポリシーのセットアップについては、[正常性ポリシーの設定\(68-7 ページ\)](#)を参照してください。

手順 2 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。すぐに適用できるデフォルト正常性ポリシーについては、[デフォルト正常性ポリシーについて\(68-8 ページ\)](#)を参照してください。

手順 3 オプションで、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。

ヘルス モニタ アラートのセットアップについては、[ヘルス モニタ アラートの設定 \(68-43 ページ\)](#)を参照してください。

システム上でヘルス モニタリングをセットアップしたら、[ヘルス モニタ (Health Monitor)] ページまたは [ヘルス イベント (Health Events)] テーブル ビューでいつでもヘルス ステータスを確認できます。システム ヘルス データの表示方法については、次のトピックを参照してください。

- [ヘルス モニタの使用 \(68-46 ページ\)](#)
- [アプライアンス ヘルス モニタの使用 \(68-48 ページ\)](#)
- [ヘルス イベントの操作 \(68-54 ページ\)](#)

正常性ポリシーの設定

ライセンス:任意 (Any)

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。正常性ポリシーで設定可能なヘルス モジュールの詳細については、[ヘルス モニタリングについて \(68-2 ページ\)](#)を参照してください。

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。別の Defense Center からエクスポートした正常性ポリシーをインポートすることもできます。

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。

Defense Center と自動的に適用されるデフォルト正常性ポリシーの詳細については、[デフォルト正常性ポリシーについて \(68-8 ページ\)](#)を参照してください。

詳細は、次のトピックを参照してください。

- [デフォルト正常性ポリシーについて \(68-8 ページ\)](#)
- [正常性ポリシーの作成 \(68-9 ページ\)](#)
- [正常性ポリシーの適用 \(68-34 ページ\)](#)
- [正常性ポリシーの編集 \(68-35 ページ\)](#)
- [正常性ポリシーの比較 \(68-37 ページ\)](#)
- [正常性ポリシーの削除 \(68-40 ページ\)](#)

デフォルト正常性ポリシーについて

ライセンス:任意(Any)

Defense Center ヘルス モニタには、アプライアンスのヘルス モニタリングの迅速な実装を容易にするデフォルト正常性ポリシーがあります。デフォルト正常性ポリシーは、自動的に Defense Center 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。詳細については、[正常性ポリシーの作成\(68-9 ページ\)](#)を参照してください。

また、デバイスの正常性を監視するために、正常性ポリシーを管理対象デバイスにプッシュすることもできます。



(注)

正常性ポリシーを Blue Coat X-Series 向け Cisco NGIPS に適用することはできません。

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。次の表に、Defense Center と管理対象デバイスのデフォルト ポリシーでアクティブにされているモジュールの詳細を示します。

表 68-2 デフォルト アクティブヘルス モジュール

モジュール	Defense Center	管理対象デバイス (Managed Device)
Advanced Malware Protection	Yes	No
アプライアンス ハートビート	Yes	No
自動アプリケーション バイパス	No	Yes
CPU 使用率(CPU Usage)	No	No
カードリセット	No	No
ディスク ステータス	Yes	Yes
ディスク使用量	Yes	Yes
FireAMP ステータス モニタ	Yes	No
FireSIGHT ホスト ライセンス制限	Yes	No
ハードウェア アラーム	No	Yes
ヘルス モニタ プロセス	No	No
インライン リンク不一致アラーム	No	Yes
インターフェイス ステータス	No	Yes
侵入イベント レート	No	Yes
ライセンス モニタ	Yes	No
リンク ステート伝達	No	Yes
メモリ使用率(Memory Usage)	Yes	Yes
電源モジュール(Power Supply)	No	Yes

表 68-2 デフォルト アクティブ ヘルス モジュール(続き)

モジュール	Defense Center	管理対象デバイス (Managed Device)
Process Status	Yes	Yes
検出の再設定	No	Yes
RRD サーバ プロセス	Yes	No
セキュリティ インテリジェンス (Security Intelligence)	Yes	No
時系列データ モニタ	Yes	No
時刻同期ステータス	Yes	Yes
URL フィルタリング モニタ	Yes	No
ユーザ エージェント ステータス モニタ	Yes	No
VPN ステータス	Yes	No

正常性ポリシーの作成

ライセンス:任意(Any)

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。



ヒント

新しいポリシーを作成する代わりに、別の Defense Center から正常性ポリシーをエクスポートして、それを対象の Defense Center にインポートできます。ニーズに合わせて、インポートされたポリシーを編集してから適用することができます。詳細については、[設定のインポートおよびエクスポート \(A-1 ページ\)](#)を参照してください。

正常性ポリシーを作成する方法:

アクセス:Admin/Maint

- 手順 1 [ヘルス (Health)] > [正常性ポリシー (Health Policy)] の順に選択します。
[正常性ポリシー (Health Policy)] ページが表示されます。
- 手順 2 [ポリシーの作成 (Create Policy)] をクリックします。
[正常性ポリシーの作成 (Create Health Policy)] ページが表示されます。
- 手順 3 [ポリシーのコピー (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。
- 手順 4 ポリシーの名前を入力します。
- 手順 5 ポリシーの説明を入力します。

手順 6 [保存(Save)] を選択して、ポリシー情報を保存します。

[正常性ポリシーの設定(Health Policy Configuration)] ページが開いて、モジュールのリストが表示されます。

手順 7 次の項の説明に従って、アプライアンスのヘルス ステータスをテストするために使用する各モジュールの設定を構成します。

- [ポリシー実行時間間隔の設定\(68-11 ページ\)](#)
- [高度なマルウェア防御モニタリングの設定\(68-12 ページ\)](#)
- [アプライアンス ハートビート モニタリングの設定\(68-12 ページ\)](#)
- [自動アプリケーション バイパス モニタリングの設定\(68-13 ページ\)](#)
- [CPU 使用率モニタリングの設定\(68-14 ページ\)](#)
- [カードリセット モニタリングの設定\(68-15 ページ\)](#)
- [ディスク ステータス モニタリングの設定\(68-16 ページ\)](#)
- [ディスク使用率モニタリングの設定\(68-16 ページ\)](#)
- [ステータス モニタリングFireAMPの設定\(68-17 ページ\)](#)
- [FireSIGHT ホスト使用量モニタリングの設定\(68-18 ページ\)](#)
- [ハードウェア アラーム モニタリングの設定\(68-19 ページ\)](#)
- [ヘルス ステータス モニタリングの設定\(68-20 ページ\)](#)
- [インライン リンク不一致アラーム モニタリングの設定\(68-21 ページ\)](#)
- [インターフェイス ステータス モニタリングの設定\(68-21 ページ\)](#)
- [侵入イベント レート モニタリングの設定\(68-22 ページ\)](#)
- [ライセンス モニタリングについて\(68-23 ページ\)](#)
- [リンク ステート伝達モニタリングの設定\(68-24 ページ\)](#)
- [メモリ使用率モニタリングの設定\(68-24 ページ\)](#)
- [電源モニタリングの設定\(68-26 ページ\)](#)
- [プロセス ステータス モニタリングの設定\(68-26 ページ\)](#)
- [検出のモニタリングの再設定の構成\(68-27 ページ\)](#)
- [RRD サーバプロセス モニタリングの設定\(68-28 ページ\)](#)
- [セキュリティ インテリジェンス モニタリングの設定\(68-29 ページ\)](#)
- [時系列データ モニタリングの設定\(68-30 ページ\)](#)
- [時刻同期モニタリングの設定\(68-30 ページ\)](#)
- [URL フィルタリング モニタリングの設定\(68-31 ページ\)](#)
- [ユーザ エージェント ステータス モニタリングの設定\(68-32 ページ\)](#)
- [VPN ステータス モニタリングの設定\(68-33 ページ\)](#)



(注) 設定を構成するときに、それぞれの [正常性ポリシーの設定(Health Policy Configuration)] ページでヘルス ステータスをテストするために実行するモジュールが有効になっていることを確認します。無効になっているモジュールは、そのモジュールを含むポリシーがアプライアンスに適用されていても、ヘルス ステータス フィードバックを生成しません。

- 手順 8 [ポリシーを保存して終了 (Save Policy and Exit)] をクリックしてポリシーを保存します。
有効にするには、それぞれのアプライアンスにポリシーを適用する必要があります。正常性ポリシーの適用方法については、[正常性ポリシーの適用 \(68-34 ページ\)](#) を参照してください。

ポリシー実行時間間隔の設定

ライセンス:任意 (Any)

正常性ポリシーのポリシー実行時間間隔を変更することによって、ヘルス テストの実行頻度を制御できます。設定可能な最大実行時間間隔は 99999 分です。



注意 5 分未満の実行時間間隔を設定しないでください。

ポリシー実行時間間隔を設定する方法:

アクセス:Admin/Maint

- 手順 1 [正常性ポリシーの設定 (Health Policy Configuration)] ページで、[ポリシー実行時間間隔 (Policy Run Time Interval)] を選択します。
[正常性ポリシーの設定 — ポリシー実行時間間隔 (Health Policy Configuration — Policy Run Time Interval)] ページが表示されます。
- 手順 2 [実行間隔 (分) (Run Interval (mins))] フィールドに、テストの自動反復の時間間隔を分単位で入力します。
- 手順 3 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。

設定を有効にするには、正常性ポリシーを該当するアプライアンスに適用する必要があります。詳細については、[正常性ポリシーの適用 \(68-34 ページ\)](#) を参照してください。

高度なマルウェア防御モニタリングの設定

ライセンス:Malware

このモジュールは、Cisco クラウドに問い合わせでネットワーク トラフィックでファイルを検出する Defense Center の機能の状態と安定性を追跡します。システムで、クラウドとの接続が中断された、接続に使用されている暗号キーが無効である、または一定のタイム フレームで検出されたファイル数が多すぎることが検出された場合は、このモジュールのステータス分類が Warning に変更され、モジュールが正常性アラートを生成します。使用している FireAMP プライベートクラウドがシスコのパブリック クラウドと通信できない場合は、プライベート クラウド自体でアラートが生成されます。詳細については、『*FireAMP Private Cloud Administration Portal User Guide*』を参照してください。



(注) Defense Center のインターネット接続が切断された場合、高度なマルウェア防御ヘルス アラートの生成に最大 30 分かかることがあります。

高度なマルウェア防御ヘルス モジュールの設定を構成する方法:

アクセス:Admin/Maint

-
- 手順 1 [正常性ポリシーの設定 (Health Policy Configuration)] ページで、[高度なマルウェア防御 (Advanced Malware Protection)] を選択します。
- [正常性ポリシーの設定 — 高度なマルウェア防御 (Health Policy Configuration — Advanced Malware Protection)] ページが表示されます。
- 手順 2 [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 テストに対するモジュールの使用を有効にします。
- 手順 3 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。

設定を有効にするには、正常性ポリシーを該当するアプライアンスに適用する必要があります。詳細については、[正常性ポリシーの適用 \(68-34 ページ\)](#) を参照してください。

アプライアンス ハートビート モニタリングの設定

ライセンス:任意 (Any)

Defense Center は、デバイスが実行しており、Defense Center と正常に通信していることを示すものとして、その管理対象デバイスから、2 分ごとと 200 イベントごとのどちらか早い方でハートビートを受け取ります。アプライアンス ハートビート ヘルス ステータス モジュールは、Defense Center が管理対象アプライアンスからハートビートを受信しているかどうかを追跡するために使用します。Defense Center がデバイスからのハートビートを検出しない場合、このモジュールのステータス分類が Critical に変わります。このステータス データがヘルス モニタに反映されます。

アプライアンス ハートビート ヘルス モジュールの設定を構成する方法:

アクセス:Admin/Maint

-
- 手順 1 [正常性ポリシーの設定 (Health Policy Configuration)] ページで、[アプライアンス ハートビート (Appliance Heartbeat)] を選択します。
[正常性ポリシーの設定 — アプライアンス ハートビート (Health Policy Configuration — Appliance Heartbeat)] ページが表示されます。
- 手順 2 [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 テストに対するモジュールの使用を有効にします。
- 手順 3 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。

設定を有効にするには、正常性ポリシーを該当するアプライアンスに適用する必要があります。詳細については、[正常性ポリシーの適用 \(68-34 ページ\)](#) を参照してください。

自動アプリケーションバイパス モニタリングの設定

ライセンス:任意 (Any)

このモジュールは、管理対象デバイスがバイパスしきい値として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時点を検出するために使用します。バイパスが発生すると、このモジュールがアラートを生成します。このステータス データがヘルス モニタに反映されます。

自動アプリケーションバイパスの詳細については、[自動アプリケーションバイパス \(4-60 ページ\)](#) を参照してください。

自動アプリケーションバイパス モニタリング ステータスを設定する方法:

アクセス:Admin/Maint

-
- 手順 1 [正常性ポリシーの設定 (Health Policy Configuration)] ページで、[自動アプリケーションバイパス ステータス (Automatic Application Bypass Status)] を選択します。
[正常性ポリシーの設定 — 自動アプリケーションバイパス ステータス (Health Policy Configuration — Automatic Application Bypass Status)] ページが表示されます。
- 手順 2 [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 テストに対するモジュールの使用を有効にします。

手順 3 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。

設定を有効にするには、正常性ポリシーを該当する管理対象デバイスに適用する必要があります。詳細については、[正常性ポリシーの適用 \(68-34 ページ\)](#) を参照してください。

CPU 使用率モニタリングの設定

ライセンス:任意 (Any)

サポートされるデバイス:任意 (3D9900 は除く)

サポートされる防御センター:任意 (Any)

CPU 使用率が高すぎる場合、ハードウェアをアップグレードする必要がある、または、正しく機能していないプロセスが存在することを示している可能性があります。CPU 使用率ヘルス ステータス モジュールは、CPU 使用率の制限を設定するために使用します。

モニタ対象アプライアンスの CPU 使用率が警告制限を超えた場合、そのモジュールのステータス分類が **Warning** に変更されます。モニタ対象アプライアンスの CPU 使用率が重大制限を超えた場合、そのモジュールのステータス分類が **Critical** に変更されます。このステータス データがヘルス モニタに反映されます。

両方の制限に設定可能な最大パーセンテージは 100 % であり、重大制限は警告制限より高くする必要があります。

CPU 使用率の制限を設定する方法:

アクセス:Admin/Maint

- 手順 1 [正常性ポリシーの設定 (Health Policy Configuration)] ページで、[CPU 使用率 (CPU Usage)] を選択します。
- [正常性ポリシーの設定 — CPU 使用率 (Health Policy Configuration — CPU Usage)] ページが表示されます。
- 手順 2 [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 テストに対するモジュールの使用を有効にします。
- 手順 3 [重大しきい値 % (Critical Threshold %)] フィールドに、重大ヘルス ステータスをトリガーする CPU 使用率のパーセンテージを入力します。
- 手順 4 [警告しきい値 % (Warning Threshold %)] フィールドに、警告ヘルス ステータスをトリガーする CPU 使用率のパーセンテージを入力します。

手順 5 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。

設定を有効にするには、正常性ポリシーを該当するアプライアンスに適用する必要があります。詳細については、[正常性ポリシーの適用 \(68-34 ページ\)](#) を参照してください。

カードリセット モニタリングの設定

ライセンス:任意 (Any)

カードリセット モニタリング ヘルス ステータス モジュールは、ハードウェア障害が原因でネットワーク カードが再起動された時点を追跡するために使用します。リセットが発生すると、このモジュールがアラートを生成します。このステータス データがヘルス モニタに反映されます。

カードリセット モニタリングを設定する方法:

アクセス:Admin/Maint

手順 1 [正常性ポリシーの設定 (Health Policy Configuration)] ページで、[カードリセット (Card Reset)] を選択します。

[正常性ポリシーの設定 — カードリセット (Health Policy Configuration — Card Reset Monitoring)] ページが表示されます。

手順 2 [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 テストに対するモジュールの使用を有効にします。

手順 3 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。

設定を有効にするには、該当する Defense Center に正常性ポリシーを適用する必要があります。詳細については、[正常性ポリシーの適用 \(68-34 ページ\)](#) を参照してください。

ディスク ステータス モニタリングの設定

ライセンス:任意(Any)

ディスク ステータス ヘルス モジュールは、アプライアンスのハードディスクとマルウェア ストレージパック(設置されている場合)の現在のステータスをモニタするために使用します。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 ステータス ヘルス モジュールの設定を構成する方法:

アクセス:Admin/Maint

-
- 手順 1** [正常性ポリシーの設定(Health Policy Configuration)] ページで、[ディスク ステータス(Disk Status)] をクリックします。
- [正常性ポリシーの設定 — ディスク ステータス(Health Policy Configuration — Disk Status)] ページが表示されます。
- 手順 2** [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 テストに対するモジュールの使用を有効にします。
- 手順 3** 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。

設定を有効にするには、正常性ポリシーを該当するデバイスに適用する必要があります。詳細については、[正常性ポリシーの適用\(68-34 ページ\)](#)を参照してください。

ディスク使用率モニタリングの設定

ライセンス:任意(Any)

十分なディスク スペースがないと、アプライアンスは動作できません。ヘルス モニタは、スペースが使い果たされる前に、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 スペースが少ない状態を特定できます。また、ヘルス モニタは、ハード ドライブのファイル ドレインが頻繁に発生する場合にアラートを出せます。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。



- (注) 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。
-

モニタ対象アプライアンスのディスク使用率が警告制限を超えた場合、そのモジュールのステータス分類が **Warning** に変更されます。モニタ対象アプライアンスのディスク使用率が重大制限を超えた場合、そのモジュールのステータス分類が **Critical** に変更されます。両方の制限に設定可能な最大パーセンテージは 100 % であり、重大制限は警告制限より高くする必要があります。

システムが未処理のイベントを削除すると、そのモジュールのステータス分類が **Warning** に変更されます。システムがモジュールしきい値に基づいて、頻繁に、ディスク使用率カテゴリ内のファイルをドレインしている場合、または、モニタ対象ディスク使用率カテゴリに含まれないファイルのディスク使用率がモジュールしきい値に基づいて大きくなる場合、そのモジュールのステータス分類が **Critical** に変更されます。ディスク使用率カテゴリの詳細については、[Disk Usage ウィジェットについて \(55-31 ページ\)](#) を参照してください。

ディスク使用率ヘルス モジュールの設定を構成する方法:

アクセス: Admin/Maint

-
- 手順 1** [正常性ポリシーの設定 (Health Policy Configuration)] ページで、[ディスク使用率 (Disk Usage)] を選択します。
- [正常性ポリシーの設定 — ディスク使用率 (Health Policy Configuration — Disk Usage)] ページが表示されます。
- 手順 2** [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 テストに対するモジュールの使用を有効にします。
- 手順 3** [重大しきい値 % (Critical Threshold %)] フィールドに、重大ヘルス ステータスをトリガーするディスク使用率のパーセンテージを入力します。
- 手順 4** [警告しきい値 % (Warning Threshold %)] フィールドに、警告ヘルス ステータスをトリガーするディスク使用率のパーセンテージを入力します。
- 手順 5** 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。

設定を有効にするには、正常性ポリシーを該当するアプライアンスに適用する必要があります。詳細については、[正常性ポリシーの適用 \(68-34 ページ\)](#) を参照してください。

ステータス モニタリング FireAMP の設定

ライセンス: 任意 (Any)

FireAMP ステータス モニタ モジュールは、次の状況でアラートを出すために使用します。

- Defense Center が Cisco クラウドに最初は正しく接続できたのに、その後接続できない。
- FireAMP ポータルを使用してクラウド接続を登録解除した
- FireAMP プライベートクラウドがシスコのパブリック クラウドと通信できない。

このようなケースでは、モジュール ステータスが **Critical** に変更され、失敗した接続に関連付けられたクラウド名が表示されます。クラウド接続の設定方法については、[FireAMP 用のクラウド接続の操作 \(37-29 ページ\)](#) を参照してください。

FireAMP ステータス モニタ モジュールの設定を構成する方法:

アクセス:Admin/Maint

-
- 手順 1** [正常性ポリシーの設定 (Health Policy Configuration)] ページで、[FireAMP ステータス モニタ (FireAMP Status Monitor)] を選択します。
- [Health Policy Configuration — FireAMP Status Monitor] ページが表示されます。
- 手順 2** [Enabled] オプションに対して [On] を選択して、FireAMP ステータス モニタリングに対するモジュールの使用を有効にします。
- 手順 3** 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。

設定を有効にするには、正常性ポリシーを **Defense Center** に適用する必要があります。詳細については、[正常性ポリシーの適用 \(68-34 ページ\)](#) を参照してください。

FireSIGHT ホスト使用量モニタリングの設定

ライセンス:FireSIGHT

FireSIGHT ホスト ライセンス制限ヘルス ステータス モジュールは、FireSIGHT ホスト使用量警告制限を設定するために使用します。モニタ対象デバイス上の残りの FireSIGHT ホスト数が警告ホスト数制限を下回った場合は、そのモジュールのステータス分類が **Warning** に変更されます。モニタ対象デバイス上の残りの FireSIGHT ホスト数が重大ホスト数制限を下回った場合は、そのモジュールのステータス分類が **Critical** に変更されます。このステータス データがヘルス モニタに反映されます。

両方の制限に設定可能な最大ホスト数は 1000 で、重大ホスト制限数は警告制限より小さくする必要があります。

FireSIGHT ホスト ライセンス制限ヘルス モジュールの設定を構成する方法:

アクセス:Admin/Maint

-
- 手順 1** [正常性ポリシーの設定 (Health Policy Configuration)] ページで、[FireSIGHT ホスト ライセンス制限 (FireSIGHT Host License Limit)] を選択します。
- [正常性ポリシーの設定 — FireSIGHT ホスト ライセンス制限 (Health Policy Configuration — FireSIGHT Host License Limit)] ページが表示されます。
- 手順 2** [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 テストに対するモジュールの使用を有効にします。

- 手順 3 [重大ステータスのホスト数(Critical number Hosts)] フィールドに、重大ヘルス ステータスをトリガーする使用可能なホストの残数を入力します。
- 手順 4 [警告ステータスのホスト数(Warning number Hosts)] フィールドに、警告ヘルス ステータスをトリガーする使用可能なホストの残数を入力します。
- 手順 5 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。

設定を有効にするには、正常性ポリシーを該当するデバイスに適用する必要があります。詳細については、[正常性ポリシーの適用\(68-34 ページ\)](#)を参照してください。

ハードウェア アラーム モニタリングの設定

ライセンス:任意(Any)

サポートされるデバイス:シリーズ 3、3D9900

ハードウェア アラーム ヘルス ステータス モジュールは、シリーズ 3 または 3D9900 デバイス上でハードウェア障害を検出するために使用します。ハードウェア アラーム モジュールが、障害が発生したハードウェア コンポーネントまたは相互に通信していないクラスタ化されたデバイスを検出すると、そのモジュールのステータス分類が **Critical** に変更されます。このステータス データがヘルス モニタに反映されます。

3D9900 デバイス上のハードウェア アラームの原因となるハードウェア ステータス状態の詳細については、[3D9900 デバイスのハードウェア アラーム詳細の解釈\(68-58 ページ\)](#)を参照してください。

ハードウェア アラーム ヘルス モジュールの設定を構成する方法:

アクセス:Admin/Maint

- 手順 1 [正常性ポリシーの設定(Health Policy Configuration)] ページで、[ハードウェア アラーム(Hardware Alarms)] を選択します。
- [正常性ポリシーの設定 — ハードウェア アラーム モニタ(Health Policy Configuration — Hardware Alarm Monitor)] ページが表示されます。
- 手順 2 [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 テストに対するモジュールの使用を有効にします。
- 手順 3 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。

設定を有効にするには、正常性ポリシーを該当するデバイスに適用する必要があります。詳細については、[正常性ポリシーの適用 \(68-34 ページ\)](#) を参照してください。

ヘルス ステータス モニタリングの設定

ライセンス:任意 (Any)

ヘルス モニタ プロセス モジュールは、monita 対象アプライアンスから受け取るヘルス イベントの時間間隔が長すぎる場合にアラートを生成することによって、Defense Center 上でのヘルス モニタの正常性をモニタするために使用します。

たとえば、Defense Center (myrtle.example.com) がデバイス (dogwood.example.com) をモニタする場合は、ヘルス モニタ プロセス モジュールが有効になっている正常性ポリシーを myrtle.example.com に適用します。その後、ヘルス モニタ プロセス モジュールが、dogwood.example.com から最後のイベントが受信されてから経過した分数を示すイベントを報告します。

アラートの生成を引き起こすイベントの時間間隔を分単位で設定できます。最後のイベント制限以降の待ち時間が [警告の分数 (Warning Minutes)] に設定された分数を超えると、そのモジュールのステータス分類が **Warning** に変更されます。最後のイベント制限以降の待ち時間が [重大の分数 (Critical Minutes)] を超えると、そのモジュールのステータス分類が **Critical** に変更されます。このステータス データがヘルス モニタに反映されます。

両方の制限に設定可能な最大分数は 144 であり、重大制限は警告制限より高くする必要があります。最小分数は 5 です。

ヘルス モニタ プロセス モジュールの設定を構成する方法:

アクセス:Admin/Maint

- 手順 1** [正常性ポリシーの設定 (Health Policy Configuration)] ページで、[ヘルス モニタ プロセス (Health Monitor Process)] を選択します。
[正常性ポリシーの設定 — ヘルス モニタ プロセス (Health Policy Configuration — Health Monitor Process)] ページが表示されます。
- 手順 2** [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 テストに対するモジュールの使用を有効にします。
- 手順 3** [重大:最終イベント以降の分数 (Critical Minutes since last event)] に、重大ヘルス ステータスをトリガーする前にイベント間で待機する最大分数を入力します。
- 手順 4** [警告:最終イベント以降の分数 (Warning Minutes since last event)] に、警告ヘルス ステータスをトリガーする前にイベント間で待機する最大分数を入力します。
- 手順 5** 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。

設定を有効にするためには、正常性ポリシーを Defense Center に適用する必要があります。詳細については、[正常性ポリシーの適用 \(68-34 ページ\)](#) を参照してください。

インライン リンク不一致アラーム モニタリングの設定

ライセンス:任意 (Any)

インライン リンク不一致アラーム ヘルス ステータス モジュールは、インライン セットの両側のインターフェイスが別々の接続速度をネゴシエートした時点を追跡するために使用します。別々にネゴシエートされた速度が検出された場合は、このモジュールがアラートを生成します。

インライン リンク不一致モニタリングを設定する方法:

アクセス:Admin/Maint

- 手順 1** [正常性ポリシーの設定 (Health Policy Configuration)] ページで、[インライン リンク不一致アラーム (Inline Link Mismatch Alarms)] を選択します。
[正常性ポリシーの設定 — インライン リンク不一致アラーム (Health Policy Configuration — Inline Link Mismatch Alarms)] ページが表示されます。
- 手順 2** [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 テストに対するモジュールの使用を有効にします。
- 手順 3** 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。

設定を有効にするには、該当する Defense Center に正常性ポリシーを適用する必要があります。詳細については、[正常性ポリシーの適用 \(68-34 ページ\)](#) を参照してください。

インターフェイス ステータス モニタリングの設定

ライセンス:FireSIGHT

インターフェイス ステータス ヘルス ステータス モジュールは、デバイスがトラフィックを受信しているかどうかを検出するために使用します。インターフェイス ステータス モジュールで、デバイスがトラフィックを受信していないことが確認されると、そのモジュールのステータス分類が Critical に変わります。このステータス データがヘルス モニタに反映されます。



(注)

DataPlaneInterface x 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 ASA 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 packets フローに関与します。

インターフェイス ステータス ヘルス モジュールの設定を構成する方法:

アクセス:Admin/Maint

- 手順 1 [正常性ポリシーの設定 (Health Policy Configuration)] ページで、[インターフェイス ステータス (Interface Status)] を選択します。
- [正常性ポリシーの設定 — インターフェイス ステータス (Health Policy Configuration — Interface Status)] ページが表示されます。
- 手順 2 [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 テストに対するモジュールの使用を有効にします。
- 手順 3 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。

設定を有効にするには、正常性ポリシーを該当するデバイスに適用する必要があります。詳細については、[正常性ポリシーの適用 \(68-34 ページ\)](#) を参照してください。

侵入イベント レート モニタリングの設定

ライセンス:Protection

侵入イベント レート ヘルス ステータス モジュールは、ヘルス ステータスの変化をトリガーする 1 秒あたりの packets 数の制限を設定するために使用します。モニタ対象デバイス上のイベント レートが [イベント数/秒 (警告) (Events per second (Warning))] 制限で設定された 1 秒あたりのイベント数を超えると、そのモジュールのステータス分類が **Warning** に変更されます。モニタ対象デバイス上のイベント レートが [イベント数/秒 (重大) (Events per second (Critical))] 制限で設定された 1 秒あたりのイベント数を超えると、そのモジュールのステータス分類が **Critical** に変更されます。このステータス データがヘルス モニタに反映されます。

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、[イベント数/秒 (重大) (Events per second (Critical))] を 50 に設定し、[イベント数/秒 (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 (Statistics)] ページ ([システム (System)] > [モニタ (Monitoring)] > [統計 (Statistics)]) で [イベント数/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。

- イベント数/秒 (重大) (Events per second (Critical)) = イベント数/秒 (Events/Sec) * 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。

侵入イベント レート モニタ ヘルス モジュールの設定を構成する方法:

アクセス:Admin/Maint

-
- 手順 1 [正常性ポリシーの設定 (Health Policy Configuration)] ページで、[侵入イベント レート (Intrusion Event Rate)] を選択します。
[正常性ポリシーの設定 — 侵入イベント レート (Health Policy Configuration — Intrusion Event Rate)] ページが表示されます。
- 手順 2 [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 テストに対するモジュールの使用を有効にします。
- 手順 3 [イベント数/秒 (重大) (Events per second (Critical))] フィールドに、重大ヘルス ステータスをトリガーする 1 秒あたりのイベント数を入力します。
- 手順 4 [イベント数/秒 (警告) (Events per second (Warning))] フィールドに、警告ヘルス ステータスをトリガーする 1 秒あたりのイベント数を入力します。
- 手順 5 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。

設定を有効にするには、正常性ポリシーを該当するデバイスに適用する必要があります。詳細については、[正常性ポリシーの適用 \(68-34 ページ\)](#) を参照してください。

ライセンス モニタリングについて

ライセンス:任意 (Any)

ライセンス モニタリング ヘルス ステータス モジュールは、Control、Protection、URL Filtering、Malware、および VPN の十分なライセンスが残っているかどうかを確認するために使用します。このモジュールは、残りのライセンスの数が少ないまたは不十分な場合にアラートを出します。

また、スタック設定内のデバイスのライセンス セットが一致しないことをシステムが検出した場合にもアラートを出します (スタックされたデバイスのライセンス セットは同じでなければなりません)。

ライセンス モニタリング モジュールは自動的に設定されます。このモジュールは変更または無効にすることができないため、[正常性ポリシーの設定 (Health Policy Configuration)] ページに表示されません。

リンク ステート伝達モニタリングの設定

ライセンス:任意(Any)

リンク ステート伝達ヘルス ステータス モジュールは、インライン ペア上のリンク ステートの伝達を検出するために使用します。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 **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。

リンク ステート伝達ヘルス モジュールの設定を構成する方法:

アクセス:Admin/Maint

手順 1 [正常性ポリシーの設定 (Health Policy Configuration)] ページで、[リンク ステート伝達 (Link State Propagation)] を選択します。

[正常性ポリシーの設定 — リンク ステート伝達 (Health Policy Configuration — Link State Propagation)] ページが表示されます。

手順 2 [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 テストに対するモジュールの使用を有効にします。

手順 3 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。

設定を有効にするには、正常性ポリシーを該当するデバイスに適用する必要があります。詳細については、[正常性ポリシーの適用 \(68-34 ページ\)](#) を参照してください。

メモリ使用率モニタリングの設定

ライセンス:任意(Any)

メモリ使用率ヘルス ステータス モジュールは、メモリ使用率の制限を設定するために使用します。このモジュールは、空きメモリ、キャッシュされたメモリ、およびスワップ メモリを考慮して空きメモリを計算します。モニタ対象アプライアンスのメモリ使用率が警告制限を超えた場合は、そのモジュールのステータス分類が **Warning** に変更されます。モニタ対象アプライアンスのメモリ使用率が重大制限を超えた場合は、そのモジュールのステータス分類が **Critical** に変更されます。このステータス データがヘルス モニタに反映されます。

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。



(注) 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、Cisco は、[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。

両方の制限に設定可能な最大パーセンテージは 100 % であり、重大制限は警告制限より高くする必要があります。



(注) 多数の FireSIGHT 機能(セキュリティ インテリジェンス、ファイル キャプチャ、複数のルールを使用した侵入ポリシー、URL フィルタリングなど)を有効にして、アクセス コントロール ポリシーを適用した場合、よりローエンドの ASA FirePOWER デバイスによっては、メモリ割り当てを最大限拡張して使用するために、断続的なメモリ使用率警告が生成される可能性があります。

メモリ使用率ヘルス モジュールの設定を構成する方法:

アクセス: Admin/Maint

- 手順 1 [正常性ポリシーの設定 (Health Policy Configuration)] ページで、[メモリ使用率 (Memory Usage)] を選択します。
- [正常性ポリシーの設定 — メモリ使用率 (Health Policy Configuration — Memory Usage)] ページが表示されます。
- 手順 2 [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 テストに対するモジュールの使用を有効にします。
- 手順 3 [重大しきい値 % (Critical Threshold %)] フィールドに、重大ヘルス ステータスをトリガーするメモリ使用率のパーセンテージを入力します。
- 手順 4 [警告しきい値 % (Warning Threshold %)] フィールドに、警告ヘルス ステータスをトリガーするメモリ使用率のパーセンテージを入力します。
- 手順 5 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。

設定を有効にするには、正常性ポリシーを該当するアプライアンスに適用する必要があります。詳細については、[正常性ポリシーの適用 \(68-34 ページ\)](#) を参照してください。

電源モニタリングの設定

ライセンス:任意(Any)

サポートされるデバイス:3D3500、3D4500、3D6500、3D9900、シリーズ 3

サポートされる防御センター:DC1500、DCDC2000、DC3500、DC4000

電源ヘルス ステータス モジュールは、サポートされているプラットフォームのいずれかで電源障害を検出するために使用します。モジュールが電力を消失した電源を検出すると、そのモジュールのステータス分類は **No Power** に変わります。モジュールが電源の存在を検出できない場合、ステータスは **Critical Error** に変わります。このステータス データがヘルス モニタに反映されます。ヘルス モニタの [アラートの詳細(Alert Detail)] リストで [電源(Power Supply)] 項目を展開して、電源ごとの特定のステータス項目を表示できます。

電源ヘルス モジュールの設定を構成する方法:

アクセス:Admin/Maint

-
- 手順 1** [正常性ポリシーの設定(Health Policy Configuration)] ページで、[電源(Power Supply)] を選択します。
- [正常性ポリシーの設定 — 電源(Health Policy Configuration — Power Supply)] ページが表示されます。
- 手順 2** [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 テストに対するモジュールの使用を有効にします。
- 手順 3** 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。

設定を有効にするには、正常性ポリシーを該当するデバイスに適用する必要があります。詳細については、[正常性ポリシーの適用\(68-34 ページ\)](#) を参照してください。

プロセス ステータス モニタリングの設定

ライセンス:任意(Any)

プロセス ステータス ヘルス モジュールは、プロセス マネージャの外部で停止または終了したアプリケーション上で実行中のプロセスをモニタするために使用します。プロセス ステータス モジュールのプロセス終了に対する応答はプロセスの終了方法によって異なります。

- プロセスがマネージャ プロセスの内部で終了した場合、モジュールはヘルス イベントを報告しません。
- 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。

プロセス ステータス ヘルス モジュールの設定を構成する方法:

アクセス:Admin/Maint

-
- 手順 1** [正常性ポリシーの設定 (Health Policy Configuration)] ページで、[プロセス ステータス (Process Status)] を選択します。
[正常性ポリシーの設定 — プロセス ステータス (Health Policy Configuration — Process Status)] ページが表示されます。
- 手順 2** [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 テストに対するモジュールの使用を有効にします。
- 手順 3** 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。

設定を有効にするには、正常性ポリシーを該当するアプライアンスに適用する必要があります。詳細については、[正常性ポリシーの適用 \(68-34 ページ\)](#) を参照してください。

検出のモニタリングの再設定の構成

ライセンス:任意 (Any)

検出モニタの再設定モジュールは、管理対象デバイスへのポリシー適用後に検出機能のステータスを確認するために使用します。ポリシーの適用に失敗して検出の機能が停止すると、モジュールはヘルス イベントでアラートを生成します。

時系列データ モニタリングの設定を構成する方法:

アクセス:Admin/Maint

-
- 手順 1** [正常性ポリシーの設定 (Health Policy Configuration)] ページで、[検出の再設定 (Reconfiguring Detection)] を選択します。
[正常性ポリシーの設定 — 検出の再設定 (Health Policy Configuration — Reconfiguring Detection)] ページが表示されます。

手順 2 [有効(Enabled)] オプションに対して [オン(On)] を選択して、ヘルス アラートに対するモジュールの使用を有効にします。

手順 3 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。

設定を有効にするには、正常性ポリシーを該当するデバイスに適用する必要があります。詳細については、[正常性ポリシーの適用\(68-34 ページ\)](#)を参照してください。

RRD サーバ プロセス モニタリングの設定

ライセンス:任意(Any)

RRD サーバ プロセス モジュールは、時系列データを保存する RRD サーバが正常に動作しているかどうかを確認するために使用します。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 Critical または Warning ステータスに遷移します。

RRD サーバ プロセス モニタリングの設定を構成する方法:

アクセス:Admin/Maint

手順 1 [正常性ポリシーの設定(Health Policy Configuration)] ページで、[RRD サーバ プロセス(RRD Server Process)] を選択します。

[正常性ポリシーの設定 — RRD サーバ プロセス(Health Policy Configuration — RRD Server Process)] ページが表示されます。

手順 2 [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 テストに対するモジュールの使用を有効にします。

手順 3 [重大:再始動回数(Critical Number of restarts)] フィールドに、重大ヘルス ステータスをトリガーする、RRD サーバ リセットの連続検出回数を入力します。

手順 4 [警告:再始動回数(Warning Number of restart)s] フィールドに、警告ヘルス ステータスをトリガーする、RRD サーバ リセットの連続検出回数を入力します。

手順 5 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。

設定を有効にするには、正常性ポリシーを該当するデバイスに適用する必要があります。詳細については、[正常性ポリシーの適用 \(68-34 ページ\)](#) を参照してください。

セキュリティ インテリジェンス モニタリングの設定

ライセンス:Protection

サポートされる防御センター:任意(DC500 を除く)

セキュリティ インテリジェンス モジュールは、セキュリティ インテリジェンス フィルタリングを伴うさまざまな状況で警告するために使用します。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。

- Defense 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
- 管理対象デバイスが Defense Center から更新されたセキュリティ インテリジェンス データを受信できない
- 管理対象デバイスが、メモリ問題のために、Defense 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ない



ヒント

セキュリティ インテリジェンス メモリ警告がヘルス モニタに表示された場合は、影響を受けるデバイスのアクセス コントロール ポリシーを再適用して、セキュリティ インテリジェンスに割り当てるメモリを増やすことができます。[アクセス コントロール ポリシーの適用 \(12-17 ページ\)](#) を参照してください。

セキュリティ インテリジェンス フィルタリングの詳細については、[セキュリティ インテリジェンスの IP アドレス レピュテーションを使用したブラックリスト登録 \(13-1 ページ\)](#) と [セキュリティ インテリジェンス リストとフィードの操作 \(3-5 ページ\)](#) を参照してください。

セキュリティ インテリジェンス モジュールの設定を構成する方法:

アクセス:Admin/Maint

- 手順 1 [正常性ポリシーの設定 (Health Policy Configuration)] ページで、[セキュリティ インテリジェンス (Security Intelligence)] を選択します。
[正常性ポリシーの設定 — セキュリティ インテリジェンス (Health Policy Configuration — Security Intelligence)] ページが表示されます。
- 手順 2 [有効 (Enabled)] オプションに対して [オン (On)] を選択して、セキュリティ インテリジェンス モニタリングに対するモジュールの使用を有効にします。
- 手順 3 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。

設定を有効にするには、正常性ポリシーを該当するデバイスに適用する必要があります。詳細については、[正常性ポリシーの適用 \(68-34 ページ\)](#) を参照してください。

時系列データ モニタリングの設定

ライセンス:任意(Any)

時系列データ モニタ モジュールは、システムが保存した時系列データ (コンプライアンス イベントのリストなど) のステータスを監視するために使用します。このモジュールは、時系列データ ストレージ ディレクトリで破損ファイルを検出します。モジュールが破損したデータを検出すると、Warning ステータスに遷移し、影響を受けるすべてのファイルの名前を報告します。

時系列データ モニタリングの設定を構成する方法:

アクセス:Admin/Maint

-
- 手順 1** [正常性ポリシーの設定 (Health Policy Configuration)] ページで、[時系列データ モニタ (Time Series Data Monitor)] を選択します。
- [正常性ポリシーの設定 — 時系列データ モニタ (Health Policy Configuration — Time Series Data Monitor)] ページが表示されます。
- 手順 2** [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 テストに対するモジュールの使用を有効にします。
- 手順 3** 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。

設定を有効にするには、正常性ポリシーを該当するデバイスに適用する必要があります。詳細については、[正常性ポリシーの適用 \(68-34 ページ\)](#) を参照してください。

時刻同期モニタリングの設定

ライセンス:任意(Any)

時刻同期ステータス モジュールは、NTP を使用して NTP サーバから時刻を取得する管理対象デバイス上の時刻がサーバ上の時刻と 10 秒以上異なる時点を検出するために使用します。

時刻同期モニタリングの設定を構成する方法:

アクセス:Admin/Maint

-
- 手順 1** [正常性ポリシーの設定 (Health Policy Configuration)] ページで、[時刻同期ステータス (Time Synchronization Status)] を選択します。
- [正常性ポリシーの設定 — 時刻同期ステータス (Health Policy Configuration — Time Synchronization Status)] ページが表示されます。
- 手順 2** [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 テストに対するモジュールの使用を有効にします。
- 手順 3** 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。

設定を有効にするには、正常性ポリシーを該当するデバイスに適用する必要があります。詳細については、[正常性ポリシーの適用 \(68-34 ページ\)](#) を参照してください。

URL フィルタリング モニタリングの設定

ライセンス:URL Filtering

サポートされる防御センター:任意 (DC500 を除く)

URL フィルタリング モニタ モジュールは、Defense Center と Cisco クラウド間の通信を追跡するために使用します。システムは、頻繁に訪問される URL に関する URL フィルタリング (カテゴリとレピュテーション) データを取得します。Defense Center がクラウドと正常に通信できない、または、クラウドから更新を取得できない場合、そのモジュールのステータス分類は Critical に変わります。

ハイ アベイラビリティ設定では、プライマリ Defense Center だけが URL フィルタリング クラウドと通信します。このモジュールからのすべてのデータはそのプライマリ アプライアンスのみを参照します。

URL フィルタリング モニタ モジュールは、Defense Center と URL フィルタリングが有効になっている管理対象デバイス間の通信も追跡します。Defense Center がクラウドと正常に通信している状態で、Defense Center が新しい URL フィルタリング データをその管理対象デバイスにプッシュできない場合、モジュール ステータスは Warning に変わります。

URL フィルタリング モニタ ヘルス モジュールの設定を構成する方法:

アクセス:Admin/Maint

-
- 手順 1** [正常性ポリシーの設定 (Health Policy Configuration)] ページで、[URL フィルタリング モニタ (URL Filtering Monitor)] を選択します。
- [正常性ポリシーの設定 — URL フィルタリング モニタ (Health Policy Configuration — URL Filtering Monitor)] ページが表示されます。
- 手順 2** [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 テストに対するモジュールの使用を有効にします。
- 手順 3** 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。

設定を有効にするには、正常性ポリシーを Defense Center に適用する必要があります。詳細については、[正常性ポリシーの適用 \(68-34 ページ\)](#) を参照してください。

ユーザ エージェント ステータス モニタリングの設定

ライセンス:FireSIGHT

ユーザ エージェント ステータス モニタ ヘルス モジュールは、Defense Center に接続されているエージェントのハートビートをモニタするために使用できます。適用した正常性ポリシー内のモジュールを有効にすると、Defense Center が Defense Center 上で設定されているエージェントのハートビートを検出しない場合に、モジュールはヘルス アラートを生成します。

ユーザ エージェント ステータス モニタ ヘルス モジュールの設定を構成する方法:

アクセス:Admin/Maint

-
- 手順 1** [正常性ポリシーの設定 (Health Policy Configuration)] ページで、[ユーザ エージェント ステータス モニタ (User Agent Status Monitor)] を選択します。
- [正常性ポリシーの設定 — ユーザ エージェント ステータス モニタ (Health Policy Configuration — User Agent Status Monitor)] ページが表示されます。
- 手順 2** [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 テストに対するモジュールの使用を有効にします。
- 手順 3** 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。

設定を有効にするには、正常性ポリシーをDefense Centerに適用する必要があります。詳細については、[正常性ポリシーの適用 \(68-34 ページ\)](#) を参照してください。

VPN ステータス モニタリングの設定

ライセンス:VPN

サポートされる防御センター:すべて(シリーズ 2 を除く)

VPN ステータス ヘルス モジュールは、設定したゲートウェイ VPN トンネルの現在のステータスをモニタするために使用します。個別のトンネルに関する情報が表示されます。このモジュールは、VPN トンネルのいずれかが動作していないときに、重大(赤色)ヘルス アラートを生成します。

VPN ステータス ヘルス モジュールの設定を構成する方法:

アクセス:Admin/Maint

- 手順 1** [正常性ポリシーの設定 (Health Policy Configuration)] ページで、[VPN ステータス (VPN Status)] をクリックします。
- [正常性ポリシーの設定 — VPN ステータス (Health Policy Configuration — VPN Status)] ページが表示されます。
- 手順 2** [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 テストに対するモジュールの使用を有効にします。
- 手順 3** 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。

設定を有効にするには、正常性ポリシーを該当するデバイスに適用する必要があります。詳細については、[正常性ポリシーの適用 \(68-34 ページ\)](#) を参照してください。

正常性ポリシーの適用

ライセンス:任意(Any)

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モニタします。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 **Defense 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。



(注)

ハイ アベイラビリティ ペア内の **Defense Center** 上で作成されたカスタム正常性ポリシーは両方のアプライアンス間で複製されます。ただし、デフォルト正常性ポリシーに対する変更は複製されません。各アプライアンスは、それ用に設定されたローカルのデフォルト正常性ポリシーを使用します。

正常性ポリシーを適用する方法:

アクセス:Admin/Maint

手順 1 [ヘルス (Health)] > [正常性ポリシー (Health Policy)] の順に選択します。

[正常性ポリシー (Health Policy)] ページが表示されます。

手順 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。

[正常性ポリシーの適用 (Health Policy Apply)] ページが表示されます。



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。

手順 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。

手順 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。

[正常性ポリシー (Health Policy)] ページが開いて、ポリシーの適用が成功したかどうかを示すメッセージが表示されます。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

ライセンス:任意(Any)

モジュールを有効または無効にするか、モジュール設定を変更することによって、正常性ポリシーを変更できます。すでにアプライアンスに適用されているポリシーを変更すると、その変更はポリシーを再適用するまで有効になりません。

さまざまなアプライアンスに適用可能なヘルス モデルを次の表に列挙します。

表 68-3 アプライアンスに適用可能なヘルス モジュール

モジュール	適用可能なアプライアンス
Advanced Malware Protection	Defense Center、DC500 以外
アプライアンス ハートビート	Defense Center
自動アプリケーションバイパス ステータス	すべての管理対象デバイス
CPU 使用率(CPU Usage)	任意(3D9900 は除く)
カードリセット	すべての管理対象デバイス
ディスク ステータス	Any
ディスク使用量	Any
FireAMP ステータス モニタ	Defense Center
FireSIGHT ホスト ライセンス制限	Defense Center
ハードウェア アラーム	シリーズ 3、3D9900
ヘルス モニタ プロセス	Defense Center
インラインリンク不一致アラーム	すべての管理対象デバイス
インターフェイス ステータス	すべての管理対象デバイス
侵入イベント レート	Protection 付きの管理対象デバイス
ライセンス モニタ	Defense Center
リンク ステート伝達	Protection 付きの管理対象デバイス
メモリ使用率(Memory Usage)	Any
電源モジュール(Power Supply)	Defense Center: DC1500、DCDC2000、DC3500、DC4000 デバイス: 3D3500、3D4500、3D6500、3D9900、シリーズ 3
Process Status	Any
検出の再設定	Any
RRD サーバ プロセス	Defense Center
セキュリティ インテリジェンス (Security Intelligence)	Defense Center、DC500 以外
時系列データ モニタ	Defense Center
時刻同期ステータス	Any
URL フィルタリング モニタ	Defense Center、DC500 以外

表 68-3 アプライアンスに適用可能なヘルス モジュール(続き)

モジュール	適用可能なアプライアンス
ユーザエージェント ステータス モニタ	Defense Center
VPN ステータス	Defense Center

正常性ポリシーを編集する方法:

アクセス:Admin/Maint

-
- 手順 1 [ヘルス (Health)] > [正常性ポリシー (Health Policy)] の順に選択します。
[正常性ポリシー (Health Policy)] ページが表示されます。
- 手順 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。
[ポリシー実行時間間隔 (Policy Run Time Interval)] 設定が選択された状態で [正常性ポリシーの設定 (Health Policy Configuration)] ページが表示されます。
- 手順 3 必要に応じて、次の項の説明に従って、設定を変更します。
- [ポリシー実行時間間隔の設定 \(68-11 ページ\)](#)
 - [高度なマルウェア防御モニタリングの設定 \(68-12 ページ\)](#)
 - [アプライアンス ハートビート モニタリングの設定 \(68-12 ページ\)](#)
 - [自動アプリケーションバイパス モニタリングの設定 \(68-13 ページ\)](#)
 - [CPU 使用率モニタリングの設定 \(68-14 ページ\)](#)
 - [カードリセット モニタリングの設定 \(68-15 ページ\)](#)
 - [ディスク ステータス モニタリングの設定 \(68-16 ページ\)](#)
 - [ディスク使用率モニタリングの設定 \(68-16 ページ\)](#)
 - [ステータス モニタリングFireAMPの設定 \(68-17 ページ\)](#)
 - [FireSIGHT ホスト使用量モニタリングの設定 \(68-18 ページ\)](#)
 - [ハードウェア アラーム モニタリングの設定 \(68-19 ページ\)](#)
 - [ヘルス ステータス モニタリングの設定 \(68-20 ページ\)](#)
 - [インライン リンク不一致アラーム モニタリングの設定 \(68-21 ページ\)](#)
 - [インターフェイス ステータス モニタリングの設定](#)
 - [侵入イベント レート モニタリングの設定 \(68-22 ページ\)](#)
 - [ライセンス モニタリングについて \(68-23 ページ\)](#)
 - [リンク ステート伝達モニタリングの設定 \(68-24 ページ\)](#)
 - [メモリ使用率モニタリングの設定 \(68-24 ページ\)](#)
 - [電源モニタリングの設定 \(68-26 ページ\)](#)
 - [プロセス ステータス モニタリングの設定 \(68-26 ページ\)](#)
 - [検出のモニタリングの再設定の構成 \(68-27 ページ\)](#)
 - [RRD サーバ プロセス モニタリングの設定 \(68-28 ページ\)](#)
 - [セキュリティ インテリジェンス モニタリングの設定 \(68-29 ページ\)](#)
 - [時系列データ モニタリングの設定 \(68-30 ページ\)](#)

- [時刻同期モニタリングの設定 \(68-30 ページ\)](#)
- [URL フィルタリング モニタリングの設定 \(68-31 ページ\)](#)
- [ユーザ エージェント ステータス モニタリングの設定 \(68-32 ページ\)](#)
- [VPN ステータス モニタリングの設定 \(68-33 ページ\)](#)

手順 4 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。

手順 5 [正常性ポリシーの適用 \(68-34 ページ\)](#) の説明に従って、該当するアプライアンスにポリシーを再適用します。

正常性ポリシーの比較

ライセンス:任意 (Any)

ポリシーの変更が組織の標準に準拠していることを確認する、または、ヘルス モニタリングのパフォーマンスを最適化するため、2 つの正常性ポリシー間の違いを調査することができます。アクセス可能な正常性ポリシーの場合、2 つの正常性ポリシーまたは同じ正常性ポリシーの 2 つのリビジョンを比較できます。アクティブな正常性ポリシーを他の正常性ポリシーとすばやく比較するには、[実行設定 (Running Configuration)] オプションを選択できます。比較した後に、必要に応じて、2 つのポリシーまたはポリシー リビジョン間の違いを記録した PDF レポートを生成できます。

正常性ポリシーまたは正常性ポリシー リビジョンを比較するための 2 つのツールが用意されています。

- 比較ビューには、2 つの正常性ポリシーまたは正常性ポリシー リビジョン間の相違点のみが並べて表示されます。各ポリシーまたはポリシー リビジョンの名前が比較ビューの左右のタイトル バーに表示されます。

これを使用して、Web インターフェイスで相違点を強調表示したまま、両方のポリシーのリビジョンを表示し移動することができます。

- 比較レポートは、正常性ポリシー レポートに類似した PDF 形式で 2 つの正常性ポリシーまたは正常性ポリシー リビジョン間の違いのみのレコードを作成します。

これを使用して、ポリシーの比較を保存、コピー、出力、共有して、さらに検証することができます。

正常性ポリシー比較ツールの知識と使い方の詳細については、以下を参照してください。

- [正常性ポリシー比較ビューの使用 \(68-38 ページ\)](#)
- [正常性ポリシー比較レポートの使用 \(68-38 ページ\)](#)

正常性ポリシー比較ビューの使用

ライセンス:任意(Any)

比較ビューは、両方の正常性ポリシーまたはポリシー リビジョンを横並び形式で表示します。各ポリシーまたはポリシー リビジョンは、比較ビューの左右のタイトルバーに表示される名前で見分けます。最終変更時刻と最終変更ユーザがポリシー名の右側に表示されます。[正常性ポリシー (Health Policy)] ページにはポリシーが最後に変更された時刻が現地時間で表示されますが、正常性ポリシー レポートでは変更時刻が UTC で表示されることに注意してください。

2 つの正常性ポリシーまたはポリシー リビジョン間の違いが強調表示されます。

- 青色は強調表示された設定が 2 つのポリシーまたはポリシー リビジョンで違うことを意味します。違いは赤色のテキストで表示されます。
- 緑色は強調表示された設定が一方のポリシーまたはポリシー リビジョンだけにあるが、他方がないことを意味します。

次の表に、実行できる操作を記載します。

表 68-4 正常性ポリシー比較ビューの操作

目的	操作
変更個別にナビゲートする	タイトルバーの上にある [前へ (Previous)] または [次へ (Next)] をクリックします。 左側と右側の間にある二重矢印アイコン(⇄)が移動し、表示している違いを示す [差異 (Difference)] 番号が変わります。
新しい正常性ポリシー比較ビューを生成する	[新しい比較 (New Comparison)] をクリックします。 [比較の選択 (Select Comparison)] ウィンドウが表示されます。詳細については、 正常性ポリシー比較レポートの使用 を参照してください。
正常性ポリシー比較レポートを生成する	[比較レポート (Comparison Report)] をクリックします。 正常性ポリシー比較レポートは比較ビューと同じ情報を含む PDF を作成します。

正常性ポリシー比較レポートの使用

ライセンス:任意(Any)

正常性ポリシー比較レポートは、正常性ポリシー比較ビューで特定された 2 つ正常性ポリシー間または同じ正常性ポリシーの 2 つのリビジョン間のすべての違いの記録を、PDF として提供するものです。このレポートは、2 つの正常性ポリシー設定間の違いをさらに調査し、その結果を保存して共有するために使用できます。

正常性ポリシー比較レポートは、アクセス可能な任意の正常性ポリシーの比較ビューから生成できます。正常性ポリシー レポートを生成する前に、未確定の変更をコミットするのを忘れないでください。コミットされた変更だけがレポートに表示されます。

設定に応じて、正常性ポリシー比較レポートに 1 つ以上のセクションを含めることができます。それぞれのセクションで、同じ形式が使用され、同じレベルの詳細が提供されます。[値 A (Value A)] 列と [値 B (Value B)] 列は、比較ビューで設定したポリシーまたはポリシーのリビジョンであることを注意してください。



ヒント

同様の手順を使用して、SSL ポリシー、ネットワーク分析ポリシー、侵入ポリシー、ファイル ポリシー、システム ポリシー、またはアクセス コントロール ポリシーを比較できます。

2 つの正常性ポリシーまたは同じポリシーの 2 つのリビジョンを比較する方法:

アクセス: Admin/Maint

-
- 手順 1** [ヘルス (Health)] > [正常性ポリシー (Health Policy)] の順に選択します。
[正常性ポリシー (Health Policy)] ページが表示されます。
- 手順 2** [ポリシーの比較 (Compare Policies)] をクリックします。
[比較の選択 (Select Comparison)] ウィンドウが表示されます。
- 手順 3** [比較対象 (Compare Against)] ドロップダウン リストから、比較するタイプを次のように選択します。
- 異なる 2 つのポリシーを比較するには、[他のポリシー (Other Policy)] を選択します。
 - 同じポリシーの 2 つのリビジョンを比較するには、[その他のリビジョン (Other Revision)] を選択します。
 - 現在のアクティブ ポリシーを他のポリシーに対して比較するには、[実行中の設定 (Running Configuration)] を選択します。

正常性ポリシー レポートを生成する前に、変更をコミットするのを忘れないでください。コミットされた変更だけがレポートに表示されます。

- 手順 4** 選択した比較タイプに応じて、次のような選択肢があります。
- 2 つの異なるポリシーを比較する場合は、[ポリシー A (Policy A)] と [ポリシー B (Policy B)] ドロップダウンリストから比較するポリシーを選択します。
 - 同じポリシーの 2 つのリビジョンを比較する場合は、[ポリシー (Policy)] ドロップダウンリストからポリシーを選択してから、[リビジョン A (Revision A)] と [リビジョン B (Revision B)] ドロップダウンリストから比較するリビジョンを選択します。
 - 現在実行されている設定を別のポリシーと比較する場合は、[ポリシー B (Policy B)] ドロップダウンリストから 2 つ目のポリシーを選択します。
- 手順 5** 正常性ポリシー比較ビューを表示するには、[OK] をクリックします。
比較ビューが表示されます。
- 手順 6** 正常性ポリシー比較レポートを生成するには、[比較レポート (Comparison Report)] をクリックします。
正常性ポリシー レポートが表示されます。ブラウザの設定によっては、レポートがポップアップ ウィンドウで表示されるか、コンピュータにレポートを保存するようにプロンプトが出されることがあります。
-

正常性ポリシーの削除

ライセンス:任意(Any)

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が無効にするまでは、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。[アラート応答の有効化と無効化\(43-8 ページ\)](#)を参照してください。



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。正常性ポリシーの作成方法については、[正常性ポリシーの作成\(68-9 ページ\)](#)を参照してください。正常性ポリシーの適用方法については、[正常性ポリシーの適用\(68-34 ページ\)](#)を参照してください。

正常性ポリシーを削除する方法:

アクセス:Admin/Maint

-
- 手順 1 [ヘルス (Health)] > [正常性ポリシー (Health Policy)] の順に選択します。
[正常性ポリシー (Health Policy)] ページが表示されます。
- 手順 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 ブラックリストの使用

ライセンス:任意(Any)

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 **Defense Center** または上のサマリ ヘルス ステータスを反映させる必要がありません。

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、**Defense 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 **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 ステータスのサマリ (Health Monitor Appliance Status Summary)] にはこのアプライアンスが **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、アプライアンス上の FireSIGHT ホスト ライセンスを使い果たした場合は、FireSIGHT ホスト ライセンス制限ステータス 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。このビューの展開方法については、[ヘルス モニタの使用 \(68-46 ページ\)](#) を参照してください。

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)

Defense 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、Defense 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。

詳細については、以下を参照してください。

- [正常性ポリシーまたはアプライアンスのブラックリストへの登録 \(68-41 ページ\)](#)
- [個別のアプライアンスのブラックリストへの登録 \(68-42 ページ\)](#)
- [個別の正常性ポリシー モジュールのブラックリストへの登録 \(68-43 ページ\)](#)

正常性ポリシーまたはアプライアンスのブラックリストへの登録

ライセンス:任意 (Any)

特定の正常性ポリシーが適用されたすべてのアプライアンスに対するヘルス イベントを無効に設定する場合、そのポリシーをブラックリストに登録できます。アプライアンス グループのヘルス モニタリングの結果を無効にする必要がある場合、そのアプライアンス グループ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、[ヘルス モニタ アプライアンス モジュールのサマリ (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 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 Disabled です。

Defense Center がハイ アベイラビリティ設定の場合は、一方のハイ アベイラビリティ ピア上の管理対象デバイスだけをブラックリストに登録できることに注意してください。ハイ アベイラビリティ ピアをブラックリストに登録することによって、それが生成したイベントとそれがヘルス イベントを受け取ったデバイスを Disabled としてマークすることもできます。ハイ アベイラビリティ ピア内の Defense Center には、ピアを完全にまたは部分的にブラックリストに登録するためのオプションがあります。

正常性ポリシー全体またはアプライアンスのグループをブラックリストに登録する方法:

アクセス:Admin/Maint

-
- 手順 1 [ヘルス (Health)] > [ブラックリスト (Blacklist)] の順に選択します。
[ブラックリスト (Blacklist)] ページが表示されます。
- 手順 2 右側にあるドロップダウン リストを使用して、リストをグループ、ポリシー、またはモデルでソートします。(Defense Center 上のグループは管理対象デバイスです。)

全部ではなく一部のヘルス モジュールがブラックリストに登録されたアプライアンスは [(部分的にブラックリストに登録) ((Partially Blacklisted))] として表示されることに注意してください。メインのブラックリスト ページでブラックリスト ステータスを編集する場合、アプライアンス上のすべてのモジュールをブラックリストに登録するか、すべてのブラックリスト登録を削除するかのいずれかを行えます。アプライアンス上の個別のヘルス モジュールをブラックリストに登録する方法については、[個別の正常性ポリシー モジュールのブラックリストへの登録 \(68-43 ページ\)](#) を参照してください。



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、Defense Center とデバイス間の通信ステータスを示します。

手順 3 以下の 2 つの対処法があります。

- 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、カテゴリを選択してから、[選択され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登録解除するには、カテゴリを選択してから、[選択されたデバイスのブラックリスト登録を解除 (Clear Blacklist on Selected Devices)] をクリックします。

ページが更新して、アプライアンスの新しいブラックリスト登録状態が表示されます。

個別のアプライアンスのブラックリストへの登録

ライセンス:任意 (Any)

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 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 [ヘルス モニタ アプライアンス モジュールのサマリ (Health Monitor Appliance Module Summary)] に 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 Disabled になります。

個別のアプライアンスをブラックリストに登録する方法:

アクセス:Admin/Maint

手順 1 [ヘルス (Health)] > [ブラックリスト (Blacklist)] の順に選択します。

[ブラックリスト (Blacklist)] ページが表示されます。

手順 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。

手順 3 以下の 2 つの対処法があります。

- 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、カテゴリを選択してから、[選択され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登録解除するには、カテゴリを選択してから、[選択されたデバイスのブラックリスト登録を解除 (Clear Blacklist on Selected Devices)] をクリックします。

ページが更新されて、アプライアンスの新しいブラックリスト登録状態が表示されます。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するには、[編集(Edit)] をクリックして、[個別の正常性ポリシー モジュールのブラックリストへの登録 \(68-43 ページ\)](#) を参照してください。

個別の正常性ポリシー モジュールのブラックリストへの登録

ライセンス:任意(Any)

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。

モジュールの一部がブラックリストに登録されている場合、そのモジュールの行は **Defense Center Web** インターフェイスにボード体で表示されます。



ヒント

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 [ヘルス モニタ アプライアンス モジュールのサマリ (Health Monitor Appliance Module Summary)] で [部分的にブラックリストに登録(Partially Blacklisted)] または [すべてのモジュールがブラックリストに登録(All Modules Blacklisted)] として表示されますが、メインの [アプライアンス ステータス サマリ (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。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。

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する方法:

アクセス:Admin/Maint

- 手順 1 [ヘルス(Health)] > [ブラックリスト(Blacklist)] の順に選択します。
[ブラックリスト(Blacklist)] ページが表示されます。
- 手順 2 グループ、ポリシー、またはモデルでソートしてから、[編集(Edit)] をクリックして、アプライアンスの正常性ポリシー モジュールのリストを表示します。
正常性ポリシー モジュールが表示されます。
- 手順 3 ブラックリストに登録するモジュールを選択します。
- 手順 4 [保存(Save)] をクリックします。

ヘルス モニタ アラートの設定

ライセンス:任意(Any)

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。

詳細は、次のトピックを参照してください。

- [ヘルス モニタ アラートの作成 \(68-44 ページ\)](#)
- [ヘルス モニタ アラートの解釈 \(68-45 ページ\)](#)
- [ヘルス モニタ アラートの編集 \(68-45 ページ\)](#)
- [ヘルス モニタ アラートの削除 \(68-46 ページ\)](#)

ヘルス モニタ アラートの作成

ライセンス:任意 (Any)

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を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、競合が通知されることに注意してください。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。

ヘルス モニタ アラートを作成する方法:

アクセス:管理

手順 1 [ヘルス (Health)] > [ヘルス モニタ アラート (Health Monitor Alerts)] の順に選択します。

[ヘルス モニタ アラート (Health Monitor Alerts)] ページが表示されます。

手順 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。

手順 3 [重大度 (Severity)] リストから、アラートをトリガーする重大度レベルを選択します。

手順 4 [モジュール (Module)] リストから、アラートを適用するモジュールを選択します。



ヒント 複数のモジュールを選択するには、Ctrl + Shift キーを押しながら、モジュール名をクリックします。

手順 5 [アラート (Alert)] リストから、選択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。



ヒント [アラート (Alerts)] をクリックして、[アラート (Alerts)] ページを開きます。アラートの作成方法については、[アラート応答の使用 \(43-2 ページ\)](#) を参照してください。

手順 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。デフォルト値は 5 分です。

ポリシー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 イベントの時間間隔の方が常に大きくなります。したがって、しきい値タイムアウトが 8 分で、ポリシー実行時間間隔が 5 分の場合、報告されるイベントの時間間隔は 10 分 (5 X 2) です。

手順 7 [保存(Save)] をクリックして、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。これで、作成したアラートが [アクティブなヘルス アラート(Active Health Alerts)] リストに表示されます。

ヘルス モニタ アラートの解釈

ライセンス:任意(Any)

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)]。
- そのテスト結果によってアラートがトリガーされたヘルス モジュールを示す [モジュール(Module)]。
- アラートをトリガーしたヘルス テスト結果を含む [説明(Description)]。

ヘルス アラートの重大度レベルの詳細については、次の表を参照してください。

表 68-5 アラートの重大度

重大度 (Severity)	説明
クリティカル (Critical)	ヘルス テスト結果が、Critical アラート ステータスをトリガーする基準を満たしました。
警告	ヘルス テスト結果が、Warning アラート ステータスをトリガーする基準を満たしました。
標準	ヘルス テスト結果が、Normal アラート ステータスをトリガー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。
Recovered	ヘルス テスト結果が Critical または Warning アラート ステータスから Normal 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 モジュールの詳細については、[ヘルス モジュールについて \(68-3 ページ\)](#) を参照してください。

ヘルス モニタ アラートの編集

ライセンス:任意(Any)

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。

ヘルス モニタ アラートを編集する方法:

アクセス:管理

-
- 手順 1 [ヘルス (Health)] > [ヘルス モニタ アラート (Health Monitor Alerts)] の順に選択します。
[ヘルス モニタ アラート (Health Monitor Alerts)] ページが表示されます。
- 手順 2 [アクティブなヘルス アラート (Active Health Alerts)] リストで、変更するアラートを選択します。
- 手順 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。
- 手順 4 必要に応じて設定を変更します。詳細については、[ヘルス モニタ アラートの作成 \(68-44 ページ\)](#)を参照してください。
- 手順 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

ライセンス:任意 (Any)

既存のヘルス モニタ アラートを削除できます。



- (注) ヘルス モニタ アラートを削除しても、関連するアラート応答は削除されません。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削除する必要があります。詳細については、[アラート応答の有効化と無効化 \(43-8 ページ\)](#)および[アラート応答の削除 \(43-8 ページ\)](#)を参照してください。
-

ヘルス モニタ アラートを削除する方法:

アクセス:管理

-
- 手順 1 [ヘルス (Health)] > [ヘルス モニタ アラート (Health Monitor Alerts)] の順に選択します。
[ヘルス モニタ アラート (Health Monitor Alerts)] ページが表示されます。
- 手順 2 [アクティブなヘルス アラート (Active Health Alerts)] リストで、削除するアラートを選択します。
- 手順 3 [削除 (Delete)] をクリックします。
アラート設定が正常に削除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 モニタの使用

ライセンス:任意 (Any)

[ヘルス モニタ (Health Monitor)] ページには、Defense Center によって管理されているすべてのデバイスに加えて、Defense 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。[ステータス (Status)] テーブルには、この Defense 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。円グラフは、各ヘルス ステータス カテゴリに含まれているアプライアンスのパーセンテージを示すヘルス ステータス内訳の別のビューを提供します。

ヘルス モニタを使用する方法:

アクセス: Admin/Maint/Any Security Analyst

- 手順 1** [ヘルス (Health)] > [ヘルス モニタ (Health Monitor)] の順にクリックします。
[ヘルス モニタ (Health Monitor)] ページが表示されます。
- 手順 2** テーブルの [ステータス (Status)] 列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、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。

以降のトピックで、[ヘルス モニタ (Health Monitor)] ページから実行可能な作業について詳しく説明します。

- [ヘルス モニタ ステータスの解釈 \(68-47 ページ\)](#)
- [アプライアンス ヘルス モニタの使用 \(68-48 ページ\)](#)
- [正常性ポリシーの設定 \(68-7 ページ\)](#)
- [ヘルス モニタ アラートの設定 \(68-43 ページ\)](#)

ヘルス モニタ ステータスの解釈

ライセンス: 任意 (Any)

次の表に示すように、重大度別に使用可能なステータス カテゴリには、Error、Critical、Warning、Normal、Recovered、および Disabled が含まれます。

表 68-6 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	ステータス色	説明
エラー (Error)		白色	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、正常に再実行され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。

表 68-6 ヘルス ステータス インジケータ (続き)

ステータス レベル	ステータス アイコン	ステータス 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 モニタの使用

ライセンス:任意 (Any)

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。



(注)

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 モニタを長期間受動的にモニタする予定の場合は、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、[ユーザ ログイン設定の管理 \(61-51 ページ\)](#) および [ユーザ インターフェイスの設定 \(63-31 ページ\)](#) を参照してください。

特定のアプライアンスのステータス サマリを表示する方法:

アクセス: Admin/Maint/Any Security Analyst

手順 1 [ヘルス (Health)] > [ヘルス モニタ (Health Monitor)] の順に選択します。
[ヘルス モニタ (Health Monitor)] ページが表示されます。

手順 2 特定のステータスを持つアプライアンスのリストを表示するには、そのステータス行内の矢印をクリックします。



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。

手順 3 アプライアンス リストの [アプライアンス (Appliance)] 列で、ヘルス モニタ ツールバー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。

[ヘルス モニタ アプライアンス (Health Monitor Appliance)] ページが表示されます。

手順 4 オプションで、[モジュール ステータス サマリ (Module 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。[アラートの詳細 (Alert Detail)] リストは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。

詳細については、次の項を参照してください。

- [ヘルス モジュールについて \(68-3 ページ\)](#)
- [ヘルス モニタ ステータスの解釈 \(68-47 ページ\)](#)
- [ステータス別のアラートの表示 \(68-49 ページ\)](#)
- [アプライアンスのすべてのモジュールの実行 \(68-49 ページ\)](#)
- [特定のヘルス モジュールの実行 \(68-50 ページ\)](#)
- [ヘルス モジュール アラート グラフの生成 \(68-51 ページ\)](#)
- [ヘルス モニタを使用したトラブルシューティング \(68-52 ページ\)](#)

ステータス別のアラートの表示

ライセンス:任意 (Any)

ステータス別にアラートのカテゴリを表示または非表示にできます。

ステータス別にアラートを表示する方法:

アクセス:Admin/Maint/Any Security Analyst

-
- 手順 1** 表示するアラートのヘルス ステータスに対応するステータス アイコンまたは円グラフの色セグメントをクリックします。そのカテゴリのアラートが [アラートの詳細 (Alert Detail)] リストに表示されます。
-

ステータス別にアラートを非表示にする方法:

アクセス:Admin/Maint/Any Security Analyst

-
- 手順 1** 表示するアラートのヘルス ステータスに対応するステータス アイコンまたは円グラフの色セグメントをクリックします。そのカテゴリの [アラートの詳細 (Alert Detail)] リスト内のアラートが非表示になります。
-

アプライアンスのすべてのモジュールの実行

ライセンス:任意 (Any)

ヘルス モジュール テストは、正常性ポリシー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ヘルス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。

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方法:

アクセス:Admin/Maint/Any Security Analyst

-
- 手順 1** [ヘルス (Health)] > [ヘルス モニタ (Health Monitor)] の順に選択します。
[ヘルス モニタ (Health Monitor)] ページが表示されます。
- 手順 2** アプライアンス リストを展開して特定のステータスの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。
-
- 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、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。
-
- 手順 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。
[ヘルス モニタ アプライアンス (Health Monitor Appliance)] ページが表示されます。
- 手順 4** [すべてのモジュールを実行 (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。ページが再び自動的に更新するのを待つこともできます。
-

特定のヘルス モジュールの実行

ライセンス:任意 (Any)

ヘルス モジュール テストは、正常性ポリシー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。

特定のヘルス モジュールを実行する方法:

アクセス:Admin/Maint/Any Security Analyst

-
- 手順 1** [ヘルス (Health)] > [ヘルス モニタ (Health Monitor)] の順に選択します。
[ヘルス モニタ (Health Monitor)] ページが表示されます。
- 手順 2** アプライアンス リストを展開して特定のステータスの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。

**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。

手順 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。

[ヘルス モニタ アプライアンス (Health Monitor Appliance)] ページが表示されます。

手順 4 [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 サマリ (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。

[アラートの詳細 (Alert Detail)] リストが展開して、そのステータス カテゴリの選択されたアプライアンスのヘルス アラートがリストされます。

手順 5 イベントのリストを表示するアラートの [アラートの詳細 (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するのを待つこともできます。

ヘルス モジュール アラート グラフの生成

ライセンス:任意 (Any)

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及ぶ結果をグラフ化できます。

ヘルス アラート モジュール グラフを生成する方法:

アクセス: Admin/Maint/Any Security Analyst

手順 1 [ヘルス (Health)] > [ヘルス モニタ (Health Monitor)] の順に選択します。

[ヘルス モニタ (Health Monitor)] ページが表示されます。

手順 2 アプライアンス リストを展開して特定のステータスの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。

**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。

手順 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。

[ヘルス モニタ アプライアンス (Health Monitor Appliance)] ページが表示されます。

- 手順 4 [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 サマリ (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。

[アラートの詳細 (Alert Detail)] リストが展開して、そのステータス カテゴリの選択されたアプライアンスのヘルス アラートがリストされます。

- 手順 5 イベントのリストを表示するアラートの [アラートの詳細 (Alert Detail)] 行で、[グラフ (Graph)] をクリックします。

一定期間のイベントのステータスを示すグラフが表示されます。グラフの下の [アラートの詳細 (Alert Detail)] セクションに、選択したアプライアンスのすべてのヘルス アラートがリストされます。



- 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。詳細については、[イベント時間の制約の設定 \(58-27 ページ\)](#) を参照してください。

ヘルス モニタを使用したトラブルシューティング

ライセンス:任意 (Any)

アプライアンスで問題が発生したときに、問題の診断に役立つように、サポートからトラブルシューティング ファイルを生成するように依頼されることがあります。次の表に示すオプションのいずれかを選択して、ヘルス モニタから報告されるトラブルシューティング データをカスタマイズすることができます。

表 68-7 選択可能なトラブルシューティング オプション

オプション	報告内容
Snort のパフォーマンスと設定 (Snort Performance and Configuration)	アプライアンス上の Snort に関連するデータと構成設定
ハードウェア パフォーマンスとログ (Hardware Performance and Logs)	アプライアンス ハードウェアのパフォーマンスに関連するデータとログ
システムの設定、ポリシー、ログ (System Configuration, Policy, and Logs)	アプライアンスの現在のシステム設定に関連する構成設定、データ、およびログ
検知機能の構成、ポリシー、ログ (Detection Configuration, Policy, and Logs)	アプライアンス上の検知機能に関連する構成設定、データ、およびログ
インターフェイスとネットワーク関連データ (Interface and Network Related Data)	アプライアンスのインラインセットとネットワーク設定に関連する構成設定、データ、およびログ
検知、認識、VDB データ、およびログ (Discovery, Awareness, VDB Data, and Logs)	アプライアンス上の現在の検出設定と認識設定に関連する構成設定、データ、およびログ
データおよびログのアップグレード (Upgrade Data and Logs)	アプライアンスの以前のアップグレードに関連するデータおよびログ
全データベースのデータ (All Database Data)	トラブルシューティング レポートに含まれるすべてのデータベース関連データ
全ログのデータ (All Log Data)	アプライアンス データベースによって収集されたすべてのログ
ネットワーク マップ情報	現在のネットワーク トポロジデータ

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

詳細については、次の項を参照してください。

- [アプライアンス トラブルシューティング ファイルの生成 \(68-53 ページ\)](#)
- [トラブルシューティング ファイルのダウンロード \(68-54 ページ\)](#)

アプライアンス トラブルシューティング ファイルの生成

ライセンス:任意 (Any)

次の手順を使用して、サポートに送信できる、カスタマイズされたトラブルシューティング ファイルを生成できます。



(注)

ハイ アベイラビリティ設定では、セカンダリ Defense Center のトラブルシューティング ファイルを生成するためにプライマリ Defense Center を使用することはできず、その逆も同様です。独自の Web インターフェイスから Defense Center のトラブルシューティング ファイルを生成する必要があります。

トラブルシューティング ファイルを生成するには、次の手順を実行します。

アクセス:Admin/Maint/Any Security Analyst

-
- 手順 1 [ヘルス (Health)] > [ヘルス モニタ (Health Monitor)] の順に選択します。
[ヘルス モニタ (Health Monitor)] ページが表示されます。
- 手順 2 アプライアンス リストを展開して特定のステータスの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。
-
- 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、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。
-
- 手順 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。
[ヘルス モニタ アプライアンス (Health Monitor Appliance)] ページが表示されます。
- 手順 4 [トラブルシューティング ファイルの生成 (Generate Troubleshooting Files)] をクリックします。
[トラブルシューティング オプション (Troubleshooting Options)] ポップアップ ウィンドウが表示されます。
- 手順 5 [全データ (All Data)] を選択して入手可能なすべてのトラブルシューティング データを生成することも、個別のチェック ボックスをオンにしてレポートをカスタマイズすることもできます。詳細については、[選択可能なトラブルシューティング オプション](#)の表を参照してください。
- 手順 6 [OK] をクリックします。
Defense Center がトラブルシューティング ファイルを生成します。タスク キュー ([システム (System)] > [モニタ (Monitoring)] > [タスク ステータス (Task Status)]) でファイル生成プロセスをモニタできます。
- 手順 7 次の項 ([トラブルシューティング ファイルのダウンロード](#)) の手順に進みます。
-

トラブルシューティング ファイルのダウンロード

ライセンス:任意(Any)

次の手順を使用して、生成されたトラブルシューティング ファイルのコピーをダウンロードします。

トラブルシューティング ファイルをダウンロードする方法には、次の手順を実行します。

アクセス:Admin/Maint/Any Security Analyst

-
- 手順 1 [システム(System)] > [モニタ(Monitoring)] > [タスク ステータス(Task Status)] の順にクリックします。
- [タスク ステータス(Task Status)] ページが表示されます。
- 手順 2 生成されたトラブルシューティング ファイルに対応するタスクを探します。
- 手順 3 アプライアンスがトラブルシューティング ファイルを生成し、タスク ステータスが [完了(Completed)] に変ったら、[クリックして生成されたファイルを取得(Click to retrieve generated files)] をクリックします。
- 手順 4 ブラウザのプロンプトに従ってファイルをダウンロードします。
- ファイルは単一の .tar.gz ファイルとしてダウンロードされます。
- 手順 5 サポートの指示に従って、トラブルシューティング ファイルをCiscoに送信してください。
-

ヘルスイベントの操作

ライセンス:任意(Any)

Defense Center には、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するための完全にカスタマイズ可能なイベント ビューがあります。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する他の情報に簡単にアクセスしたりできます。

ヘルス イベント ビュー ページで実行可能なさまざまな機能がすべてのイベント ビュー ページで一貫しています。これらの一般的な手順の詳細については、[ヘルスイベント ビューについて \(68-55 ページ\)](#) を参照してください。

[ヘルス(Health)] > [ヘルスイベント(Health Events)] メニュー オプションで、ヘルスイベントを表示したり、特定のイベントを検索したりできます。

イベントの表示について詳しくは、次の項を参照してください。

- [ヘルスイベント ビューについて \(68-55 ページ\)](#) では、FireSIGHT が生成するイベントの種類について説明します。
- [ヘルスイベントの表示 \(68-55 ページ\)](#) では、[イベント ビュー(Event View)] ページへのアクセス方法と使用方法について説明します。
- [ヘルスイベントの検索 \(68-62 ページ\)](#) では、[イベント検索(Event Search)] ページを使用して特定のイベントを検索する方法について説明します。

ヘルス イベント ビューについて

ライセンス:任意 (Any)

Defense Center ヘルス モニタはヘルス イベントを記録し、記録されたヘルス イベントは [ヘルス イベント ビュー (Health Event View)] ページで表示できます。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 イベントを生成するヘルス モジュールのタイプの詳細については、[ヘルス モジュールについて \(68-3 ページ\)](#) を参照してください。

ヘルス イベントの表示方法と検索方法については、次の項を参照してください。

- [ヘルス イベントの表示 \(68-55 ページ\)](#)
- [ヘルス イベント テーブルについて \(68-61 ページ\)](#)
- [ヘルス イベントの検索 \(68-62 ページ\)](#)

ヘルス イベントの表示

ライセンス:任意 (Any)

ヘルス モニタによって収集されたアプライアンス ヘルス データはさまざまな方法で表示できます。詳細は、次のトピックを参照してください。

- [すべてのステータス イベントの表示 \(68-55 ページ\)](#)
- [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 \(68-56 ページ\)](#)
- [ヘルス イベント テーブル ビューの操作 \(68-57 ページ\)](#)
- [3D9900 デバイスのハードウェア アラート詳細の解釈 \(68-58 ページ\)](#)
- [シリーズ 3 デバイスのハードウェア アラート詳細の解釈 \(68-59 ページ\)](#)

すべてのステータス イベントの表示

ライセンス:任意 (Any)

[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、選択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。このページに表示されるイベントを生成したヘルス モジュールについては、[ヘルス モジュールについて \(68-3 ページ\)](#) を参照してください。

Defense 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。

すべての管理対象アプライアンス上のすべてのステータス イベントを表示する方法:

アクセス: Admin/Maint/Any Security Analyst

-
- 手順 1 [ヘルス (Health)] > [ヘルス イベント (Health Events)] の順に選択します。
[イベント (Events)] ページが開いて、すべてのヘルス イベントが表示されます。



- (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。詳細については、[イベント時間の制約の設定 \(58-27 ページ\)](#) を参照してください。
-



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。詳細については、[イベント時間の制約の設定 \(58-27 ページ\)](#) を参照してください。

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

ライセンス:任意 (Any)

特定のアプライアンス上の特定のヘルス モジュールによって生成されたイベントを問い合わせることができます。

特定のモジュールのヘルス イベントを表示する方法:

アクセス:Admin/Maint/Any Security Analyst

-
- 手順 1 [ヘルス (Health)] > [ヘルス モニタ (Health Monitor)] の順に選択します。
[ヘルス モニタ (Health Monitor)] ページが表示されます。
- 手順 2 アプライアンス リストを展開して特定のステータスの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。



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、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。

-
- 手順 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。
[ヘルス モニタ アプライアンス (Health Monitor Appliance)] ページが表示されます。
- 手順 4 [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 サマリ (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。
[アラートの詳細 (Alert Detail)] リストが展開して、そのステータス カテゴリの選択されたアプライアンスのヘルス アラートがリストされます。
- 手順 5 イベントのリストを表示するアラートの [アラートの詳細 (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選択したヘルス アラート モジュールの名前を含むクエリのクエリ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。詳細については、[イベント時間の制約の設定 \(58-27 ページ\)](#) を参照してください。
- 手順 6 選択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 ビューの操作

ライセンス:任意 (Any)

次の表に、[イベント ビュー (Event View)] ページから実行可能な各操作の説明を示します。

表 68-8 ヘルス イベント ビューの機能

目的	操作
ヘルス イベント ビューに表示される列の内容を確認する	ヘルス イベント テーブルについて (68-61 ページ) で詳細を参照してください。
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する	イベント時間の制約の設定 (58-27 ページ) で詳細を参照してください。 イベント ビューを時間によって制約している場合は、(グローバルかイベントに特有かに関係なく) 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。
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列を変更する、または表示するイベントを制限する	ドリルダウン ワークフロー ページのソート (58-39 ページ) で詳細を参照してください。
ヘルス イベントを削除する	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。現在制限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。
イベント ビュー ページ間を移動する	ワークフロー内の他のページへのナビゲート (58-40 ページ) で詳細を参照してください。
他のイベント テーブルに移動して関連イベントを表示する	ワークフロー間のナビゲート (58-41 ページ) で詳細を参照してください。
すぐに再表示できるように、現在のページをブックマークする	[このページをブックマーク (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。詳細については、 ブックマークの使用 (58-42 ページ) を参照してください。
ブックマークの管理ページへ移動する	イベント ビューで [ブックマークの表示 (View Bookmarks)] をクリックします。詳細については、 ブックマークの使用 (58-42 ページ) を参照してください。
テーブル ビュー内のデータに基づいてレポートを生成する	[レポート デザイナ (Report Designer)] をクリックします。詳細については、 イベント ビューからのレポート テンプレートの作成 (57-10 ページ) を参照してください。
別のヘルス イベント ワークフローを選択する	[(ワークフローの切り替え) ((switch workflow))] をクリックします。詳細については、 ワークフローの選択 (58-19 ページ) を参照してください。
1 つのヘルス イベントに関連付けられた詳細を表示する	イベントの左側にある下矢印リンクをクリックします。
複数のヘルス イベントのイベント詳細を表示する	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から、[表示 (View)] をクリックします。

表 68-8 ヘルスイベントビューの機能(続き)

目的	操作
ビュー内のすべてのイベントのイベント詳細を表示する	[すべて表示(View All)] をクリックします。
特定のステータスのすべてのイベントを表示する	そのステータスを持つイベントの [ステータス(Status)] 列内のステータス アイコンをクリックします。

3D9900 デバイスのハードウェア アラート詳細の解釈

ライセンス:任意(Any)

3D9900 デバイス モデルでは、次の表に示すイベントにตอบสนองしてハードウェア アラームが生成されます。トリガー条件はアラートのメッセージ詳細で見つけることができます。

表 68-9 3D9900 デバイスのモニタ対象条件

モニタ対象条件	黄色または赤色エラー状態の原因
NFE カードの存在	アプライアンスに対して無効な NFE ハードウェアが検出されると、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 カードの存在への参照が追加されます。
NFE 温度	NFE 温度が 95 °C 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 温度への参照が追加されます。 NFE 温度が 99 °C 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が追加されます。
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が追加されます。
LBIM の存在	ロード バランシング インターフェイス モジュール (LBIM) スイッチ 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 LBIM の存在への参照が追加されます。
Scmd デーモン	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。
Ps1s デーモン	Ps1s 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。

表 68-9 3D9900 デバイスのモニタ対象条件(続き)

モニタ対象条件	黄色または赤色エラー状態の原因
Ftwo デーモン	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。
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が追加されます。

シリーズ 3 デバイスのハードウェア アラート詳細の解釈

シリーズ 3 デバイスでは、次の表に示すイベントにตอบสนองしてハードウェア アラームが生成されます。トリガー条件がアラートのメッセージ詳細に表示されます。

表 68-10 シリーズ 3 デバイスのモニタ対象条件

モニタ対象条件	黄色または赤色エラー状態の原因
クラスタ ステータス	クラスタ化された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。

表 68-10 シリーズ 3 デバイスのモニタ対象条件(続き)

モニタ対象条件	黄色または赤色エラー状態の原因
NFE 温度	NFE 温度が 97 °C 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 °C 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、Warning の場合は黄色を、Critical 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。
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。

ヘルスイベントテーブルについて

ライセンス:任意(Any)

Defense Center のヘルス モニタを使用して、FireSIGHT システム内の重要な機能のステータスを確認できます。ハードウェア ステータスやソフトウェア ステータスなどのさまざまな側面を監視するため正常性ポリシーを作成してアプライアンスに適用します。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。ヘルス モニタリングの詳細については、[システムのモニタリング \(67-1 ページ\)](#)を参照してください。

ヘルスイベントテーブル内のフィールドについて、次の表で説明します。

表 68-11 ヘルスイベントフィールド

フィールド	説明
テスト名 (Test Name)	イベントを生成したヘルス モジュールの名前。ヘルス モジュールのリストについては、 ヘルス モジュール を参照してください。
時刻 (Time)	ヘルスイベントのタイムスタンプ。
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 Defense 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 Defense 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 (Critical、Yellow、Green、または Disabled)。
Device	ヘルスイベントが報告されたアプライアンス。

ヘルスイベントのテーブルビューを表示する方法:

アクセス: Admin/Maint/Any Security Analyst

手順 1 [ヘルス (Health)] > [ヘルスイベント (Health Events)] の順に選択します。

テーブルビューが表示されます。ヘルスイベントの操作方法については、[ヘルスイベントの操作 \(68-54 ページ\)](#)を参照してください。



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。

ヘルス イベントの検索

ライセンス:任意(Any)

特定のヘルス イベントを検索できます。実際のネットワーク環境に合わせてカスタマイズされた検索を作成して保存すると、あとで再利用できます。次の表に、使用可能な検索基準の説明を示します。

表 68-12 ヘルス イベントの検索基準

検索フィールド(Search Field)	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るはずですが。
値	表示するイベントのヘルス テストから得られた結果の値(単位数)を指定します。 たとえば、値として 15 を指定し、[単位(Units)] フィールドに「cpu」と入力した場合は、テストの実行時点でアプライアンス CPU が 15 % の使用率で動作していたイベントが取得されます。
説明	表示するイベントの説明を指定します。たとえば、プロセスが実行できなかったヘルス イベントを表示するには、「Unable to Execute」と入力します。このフィールドでアスタリスク(*)を使用してワイルドカード検索を作成できます。
単位	表示するイベントのヘルス テストから得られた結果の単位記述子を指定します。このフィールドでアスタリスク(*)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、[単位(Units)] フィールドに「%」と入力した場合は、ディスク使用率モジュールの [単位(Units)] フィールドに「%」というラベルが付けられる(そして追加のテキストがない)ため、ディスク使用率モジュールに関するすべてのイベントが取得されます。ただし、[単位(Units)] フィールドに「*%」と入力した場合は、[単位(Units)] フィールド内のテキストの最後に「%」記号が付いているモジュールに関するすべてのイベントが取得されます。
ステータス(Status)	表示するヘルス イベントのステータスを指定します。有効なステータス レベルは、Critical、Warning、Normal、Error、および Disabled です。 たとえば、Critical ステータスを示すすべてのヘルス イベントを取得するには、「Critical」と入力します。
Device	検索を 1 つ以上の特定のデバイスによって生成されたヘルス イベントに制限するには、デバイス名か IP アドレス、またはデバイス グループ名、スタック名、またはクラスタ名を入力します。検索での FireSIGHT システムによるデバイス フィールドの処理方法については、 検索でのデバイスの指定(60-7 ページ) を参照してください。

特殊な検索構文や検索の保存とロードに関する情報を含む検索の詳細については、[検索設定の実行と保存\(60-1 ページ\)](#)を参照してください。

ヘルス イベントを検索する方法:

アクセス: Admin/Maint/Any Security Analyst

-
- 手順 1** [分析(Analysis)] > [検索(Search)] を選択します。
[検索(Search)] ページが表示されます。
- 手順 2** テーブルのドロップダウンリストから [ヘルス イベント(Health Events)] を選択します。
ページが適切な制約によって更新されます。
- 手順 3** 表 [ヘルス イベントの検索基準](#) に記載されているように、該当するフィールドに検索基準を入力します。
複数の基準を入力した場合は、すべての基準を満たすレコードだけが検索で返されます。
- 手順 4** 必要に応じて検索を保存する場合は、[プライベート(Private)] チェックボックスをオンにしてプライベートとして検索を保存すると、本人だけがアクセスできるようになります。本人のみではなくすべてのユーザを対象にする場合は、このチェックボックスをオフのままにして検索を保存します。



ヒント カスタム ユーザ ロールのデータの制限として検索を使用する場合は、必ずプライベート検索として保存する**必要**があります。

- 手順 5** 必要に応じて、後で再度使用する検索を保存できます。次の選択肢があります。
- [保存(Save)] をクリックして、検索条件を保存します。
新しい検索の場合、ダイアログボックスに検索の名前を要求するプロンプトが表示されます。一意の検索名を入力して [保存(Save)] をクリックします。保存済みの既存の検索で新しい条件を保存する場合、プロンプトは表示されません。検索が保存され([プライベート(Private)] を選択した場合は本人のアカウントでのみ閲覧可能)、後で実行できます。
 - 新しい検索を保存するか、以前保存した検索を変更して作成した検索に名前を割り当てるには、[新規として保存(Save as New)] をクリックします。
ダイアログボックスに検索の名前を要求するプロンプトが表示されます。一意の検索名を入力して [保存(Save)] をクリックします。検索が保存され([プライベート(Private)] を選択した場合は本人のアカウントでのみ閲覧可能)、後で実行できます。
- 手順 6** 検索を開始するには、[検索(Search)] ボタンをクリックします。
現在の時刻範囲に制限された検索結果がデフォルトヘルス イベント ワークフローに表示されます。カスタム ワークフローを含む別のワークフローを使用するには、[ワークフロー切り替え(switch workflow)] をクリックします。別のデフォルト ワークフローの指定方法については、[イベント ビュー設定の設定\(71-3 ページ\)](#)を参照してください。
-

