CHAPTER 12

Performance Monitor の管理

ネットワークを効果的に管理するには、ミッションクリティカルなシステムで発生するイベントをできるだけ迅速に識別し、解決する必要があります。

Performance Monitor の管理オプションでは、イベント検出を設定し、公式に基づくしきい値とユーザ設定しきい値に従って、イベントを事前に識別して表示し、ログに記録できます。

次の表に、Performance Monitor からアクセスする管理オプションを示します。

表 12-1　Performance Monitor の管理オプション

オプション	説明
Notifications	パフォーマンス イベントまたは障害が発生した場合の SNMP トラップ、Syslog エントリ、または E メールからのモニタ対象サービスの通知を設定し、イネーブルにします。「通知の操作」（P.12-1）を参照してください。
Events	あらゆる優先順位のパフォーマンス イベントまたは障害イベントを生成するためのしきい値を設定し、イネーブルにします。「イベントしきい値の操作」（P.12-7）を参照してください。
System Parameters	使用できるデータ タイプのポーリング間隔とトランケーション間隔を設定し、イネーブルにします。「システム パラメータの操作」（P.12-9）を参照してください。
Logs	デバッグ ログ ファイルを表示してエクスポートしたり、切断された RAS ユーザ セクションの概要を表示します。「ログの操作」（P.12-10）を参照してください。
My Profile	Performance Monitor の起動時にデフォルトで表示されるページを選択します。「デフォルト ページの選択」（P.12-12）を参照してください。

通知の操作

Performance Monitor では、重要な条件がグローバルに、または特定のサービスに対して定義したパフォーマンス パラメータに達するか、または超えた場合に、自動的に通知できます。
Performance Monitor では、設定した各通知タイプに個別の通知を送信します。

ここでは、通知およびその設定方法について説明します。

サポートされる SNMP トラップと Syslog メッセージについて

通知のためには、SNMP トラップ、Syslog メッセージ、およびデバイス ポーリングによって情報を提供するモニタ対象デバイスから、Performance Monitor が重要な情報を受信する必要があります。詳細については、「SNMP トラップの受信」（P.2-17）を参照してください。

Performance Monitor では、次の種類の SNMP トラップを処理できます。

ソース デバイス	サポートされる SNMP トラップと Syslog メッセージ
ASA デバイス	• ASA-4-113019 • ASA-7-713052
CSM サービス モジュール	• 実サーバの状態遷移 • インターフェイスの運用状態
VPN サービス モジュール	• 追加されたポリシー • 削除されたポリシー • 追加されたクリプト マップ • 削除されたクリプト マップ • 接続されたクリプト マップ • 接続解除されたクリプト マップ • トンネルの開始 • トンネルの停止 • インターフェイスの運用状態
VPN ルータ	• 追加されたポリシー • 削除されたポリシー • 追加されたクリプト マップ • 削除されたクリプト マップ • 接続されたクリプト マップ • 接続解除されたクリプト マップ • トンネルの開始 • トンネルの停止 • インターフェイスの運用状態

Performance Monitor では、次の種類の Syslog メッセージを処理できます。

ソース デバイス	サポートされる Syslog メッセージのタイプ
VPN 3000 コンセントレータ	• IKE-5-120 • AUTH-5-28
PIX ファイアウォール	• PIX-1-104001 • PIX-1-105006 • PIX-1-105007 • PIX-1-101001 • PIX-1-1011002 • PIX-1-101004 • PIX-2-709007 • PIX-3-201008 • PIX-3-202001 • PIX-4-113019 • PIX-7-713052
ファイアウォール サービス モジュール	• PIX-1-105006 • PIX-1-105007 • PIX-1-101001 • PIX-1-1011002 • PIX-1-101004 • PIX-2-709007 • PIX-3-201008 • PIX-3-202001 • FWSM-4-113019 • FWSM-7-713052

通知の設定

Performance Monitor では、重要な条件がグローバルに、または特定のサービスに対して定義したパフォーマンス パラメータに達するか、または超えた場合に、自動的に通知できます。
Performance Monitor では、設定した各通知タイプに個別の通知を送信します。

次の 3 つの通知レベルがあります。

- Global：すべてのサービス タイプのすべてのイベント。
- Service：1 つのサービス タイプのすべてのイベント。
- Event：特定のサービス タイプの特定のイベント。

（注）　グローバルに通知を設定し、サービス レベルまたはイベント レベルで重複している場合は、通知を重複して受信します。また、イベントレベルで通知を設定し、それがサービス レベルで設定した通知設定と重複している場合も、通知を重複して受信します。

始める前に

- CiscoWorks Common Services で E メール サーバを使用するように設定していることを確認します。「E メール使用のための Common Services の設定」（P.2-16）を参照してください。
- 通知を設定するための適切な権限を持っていることを確認します。「ユーザの権限について」（P.3-2）を参照してください。

手順

ステップ 1　[Admin] > [Notifications] を選択します。

ステップ 2　設定する通知のタイプをツリーで選択します。

- [Global]：Global 通知を設定します。
- サービス タイプ（[Firewall]、[Load Balancing]、[Remote Access VPN]、[SSL]、[Site-to-Site VPN]）：サービスのすべてのイベント タイプに対して通知を設定します。
- サービス タイプ内のイベント タイプ（ツリーの一番下のノード、たとえば、[CPU Usage]）：特定のイベント タイプだけの通知を設定します。「通知がサポートされるイベント タイプについて」（P.12-5）を参照してください。

ヒント　ツリーでの選択内容で画面が更新されますが、選択内容はツリーで維持されません。設定する通知の種類を確認するには、[Email Recipients] リストの上にある右側のペインでタイトルを確認する必要があります。このタイトルには、[Global Notifications]、[Service Notifications: *Service Type*]、[Event Notifications: *Event Type*] などと表示されます。

ステップ 3　表 12-2 に示すいずれかのタスクを実行します。

通知の設定手順

表 12-2　通知の設定手順

タスク	手順
E メールの受信者を追加する。	1. [Email Recipients] 領域で、[Add] をクリックします。 2. [Edit Email Recipients] ウィンドウで、[Email Address] テキスト ボックスに E メール アドレスを 1 つ入力します。 3. E メール メッセージを送信するイベントの重大度の範囲を定義します。[From Priority] リストと [To Priority] リストでオプションを選択します。[P1] は重大度が高い問題、[P5] は重大度が低い問題で、[OK] は解決した問題です。[From] 領域での重大度レベルの選択は、[To] 領域でのレベル選択よりも低くする必要があります。 4. [Apply] をクリックします。[Edit Email Recipients] ウィンドウが閉じます。[Notifications] ページが更新され、定義した受信者が [Email Recipients] リストに表示されます。

表 12-2　通知の設定手順（続き）

タスク	手順
SNMP トラップの受信者を追加する。	1. [Trap Recipients] 領域で、[Add] をクリックします。 2. [Edit Trap Recipients] ウィンドウで、[Host] テキスト ボックスに管理対象のデバイス IP アドレスまたは DNS ホスト名を入力します。 3. [Port] テキスト ボックスに、デバイスの [SNMP] ポート番号を指定します。 4. [Community] テキスト ボックスに、デバイスの read コミュニティ ストリングを指定します。 5. [Apply] をクリックします。[Edit Trap Recipients] ウィンドウが閉じます。[Notifications] ページが更新され、定義した受信者が [Trap Recipients] リストに表示されます。
Syslog の受信者を追加する。	1. [Syslog Recipients] 領域で、[Add] をクリックします。 2. [Edit Syslog Recipients] ウィンドウで、[Host] テキスト ボックスに Syslog ホスト名または IP アドレスを 1 つ入力します。 3. [Port] テキスト ボックスに、デバイスのポート番号を指定します。 4. [Apply] をクリックします。[Edit Syslog Recipients] ウィンドウが閉じます。[Notifications] ページが更新され、定義した受信者が [Syslog Recipients] リストに表示されます。
受信者を編集する。	1. 編集する受信者を選択し、その領域の [Edit] ボタンをクリックします。 2. 必要に応じて設定を変更し、[Apply] をクリックします。
受信者を削除する（通知をディセーブル）。	削除する受信者を選択し、その領域の [Delete] ボタンをクリックします。 **（注）**　削除はすぐに反映されます。元に戻す機能はありません。
イベント タイプごとのしきい値を設定する。	特定のイベント タイプを選択すると、受信者リストの下にある [Threshold] ボタンをクリックして、イベントの通知のしきい値を設定できます。しきい値の設定の詳細については、「イベントしきい値の操作」（P.12-7）を参照してください。

通知がサポートされるイベント タイプについて

通知では 40 種類を超えるイベント タイプがサポートされ、サービス タイプごとに分類されます（表 12-3 を参照してください）。

表 12-3　通知のイベント タイプ

モニタ対象のサービス	サポートされるイベント タイプ
ファイアウォール	CPU Usage
	Command Replication
	Device Accessible via Https
	Device Accessible via Snmp
	Failover
	Failover Cable
	Fragment Size
	HA Other
	Interface State
	Memory Usage
	New Connections
	Regular Translation
	Translation Slot
ロード バランシング	Connection Failure
	Created Connection Rate
	Dropped Connection
	Interface Status
	Real Server Status
リモート アクセス VPN	Bandwidth Usage
	CPU Usage
	Device Accessible via Snmp
	Device Load
	Inbound Connection Failures
	Interface Status
	Packet Drop
	SEP Module Packet Drop
	SEP Module Status
SSL	CPU Usage
	Device Accessible via Https
	Memory Usage
	SSL Errors

表 12-3　通知のイベント タイプ（続き）

モニタ対象のサービス	サポートされるイベント タイプ
サイト間 VPN	CPU Usage Connection Failures Crypto Map Binding Crypto Map Change Crypto Packet Drops Device Accessible via Https Device Accessible via Snmp ISAKMP Policy Change Interface Status Memory Usage Packet Drop Tunnel Status 次のすべてを実行した場合、DMVPN スポークツースポーク トンネルに関する大量の E メールを受信する可能性があります。 • スポーク間セッションをサポートするフル メッシュ トポロジを使用するように、DMVPN を設定する。 • サイト間 VPN トンネル ダウン イベントのしきい値を設定する。 • これらのイベントの自動 E メール通知をスケジューリングする。 サイト間トンネルはダイナミックで、多数のトンネル ダウン イベントが含まれる設計により、存続期間が短くなります。この大量の E メールの問題が発生する場合は、E メールの通知をディセーブルにするか、ハブだけをモニタするように Performance Monitor を設定することを推奨します。

イベントしきい値の操作

しきい値を作成するには、次のことを実行します。

- 特定のサービスのパフォーマンス メトリックまたは障害のメトリックに動作状態の境界（OK、Degraded、Overloaded など）を定義します。
- レコードが更新される前に動作状態が再帰する必要がある連続ポーリング サイクルの数を指定します。
- 特定のメトリックに対して可能性のあるそれぞれの動作状態に優先度レベルを関連付けます（表示およびユーザ通知のため）。

定義したしきい値でさまざまなサービス、メトリック、および状態を使用しますが、すべてのしきい値の定義で同じ基本ワークフローに従います。

ヒント　状態が定義したしきい値を超えるか下回ると、Performance Monitor でアラームが記録されます。アラームは対応するイベント ブラウザで表示および解釈できます。場合によっては、[Critical Problems] の要約で重大な問題も表示できます。「イベント ブラウザの操作」（P.3-12）および「クリティカルな問題の要約の操作」（P.4-2）を参照してください。

始める前に

このオプションを使用するための適切な権限を持っていることを確認します。「ユーザの権限について」（P.3-2）を参照してください。

手順

ステップ 1　[Admin] > [Events] を選択します。

ステップ 2　TOC からサービスを選択します。

（注）　インスペクション ポリシーで設定されている場合、[Firewall Devices] ページに IOS ルータが表示されますが、[Admin] > [Events] からサイト間 VPN を選択して、ルータのイベントしきい値を設定する必要があります。[Threshold Configuration] ページからファイアウォール サービスのイベントしきい値を設定しても、ルータに適用されません。

ステップ 3　しきい値を設定するパフォーマンス メトリックまたは障害のメトリックが見つかるまで、[Events] リストのエントリをスキャンし、対応する行のオプション ボタンを選択します。

ステップ 4　[Threshold] をクリックします。

ヒント　また、[Admin] > [Notifications] を選択し、イベントを選択して [Threshold] をクリックすると、イベントのしきい値を設定することもできます。

[Threshold Configuration] ページが表示されます。

- 障害のメトリックを選択した場合、[Threshold Configuration] ページに 2 つの相反する [State Name] 値（たとえば、[Up] と [Down]）が表示されます。または、1 つの極端な状態値（[OK] など）の後に、複数の中間のステータスが続きます。
- パフォーマンス メトリックを選択した場合、[State Name] 値の範囲（[OK]、[Medium]、[High] など）が [Threshold Configuration] ページに表示されます。各値は範囲内の上限のパーセンテージと下限のパーセンテージに関連付けられます。

ステップ 5　[Enable] チェックボックスをオンにします。

[Enable] チェックボックスをオンにする必要があります。そうしないと、[Threshold Configuration] ページで値を定義できません。

ステップ 6　次のいずれかを実行します。

- [State Name] 領域に 2 つの相反する値（たとえば、良好な [Up] と、問題がある [Down]）が表示される場合、次の内容を指定します。
  - 問題がある状態のイベントの優先度レベル。
  - トリガーするポーリング間隔の失敗数、クリアする成功の回数、[Repetitions before State Change] フィールドの問題のある状態に関連付けられたイベント。
- [State Name] 領域に 3 つの値の範囲が表示された場合は、上限と下限のしきい値パーセンテージ、ポーリング間隔の回数、範囲内の 3 つの値のそれぞれの優先度レベルを指定します。たとえば、中間の状態の下限のしきい値の境界として 10% を選択します（この場合、選択内容が開始状態の上限しきい値パーセンテージとして自動的に適用されます）。

（注）　パフォーマンス メトリックのしきい値を設定する場合、開始状態の下限しきい値パーセンテージは常にゼロ（0%）で、優先度は常に [OK] です。問題のある状態の上限のしきい値パーセンテージは常に 100% です。これらの値は変更できません。

ステップ 7　次のいずれかを実行します。

- 選択内容を破棄して [Events] ページに戻るには、[Cancel] をクリックします。
- 選択内容を保存して実装するには、[Apply] をクリックします。
- すべての値をデフォルト設定にリセットし、[Threshold Configuration] ページを表示したままにするには、[Default] をクリックします。

システム パラメータの操作

ポーリング間隔、トランケーション間隔、およびユーザ セッション データの保存を設定できます。

始める前に

このオプションを使用するための適切な権限を持っていることを確認します。「ユーザの権限について」（P.3-2）を参照してください。

手順

ステップ 1　[Admin] > [System Parameters] を選択します。

ステップ 2　表 12-4 に示すように、必要な設定を行います。次の表に、各設定で許可された最小値と最大値、設定のデフォルトを示します。すべての値をデフォルトに戻すには、[Default] ボタンをクリックします。

システム パラメータ

表 12-4　システム パラメータの設定

行の名前	オプション タスク	手順
Polling Interval (mins)	ポーリング間隔を設定します。	ポーリング間隔を分単位で指定するオプションをリストから選択し、[Apply] をクリックします。
Hourly aggregated data is kept for (days)	時間ごとのデータのトランケーション間隔を設定します。	時間ごとのデータを保持する日数を指定するオプションをリストから選択し、[Apply] をクリックします。
Daily aggregated data is kept for (days)	日ごとのデータのトランケーション間隔を設定します。	日ごとのデータを保持する日数を指定するオプションをリストから選択し、[Apply] をクリックします。
Weekly aggregated data is kept for (days)	週ごとのデータのトランケーション間隔を設定します。	週ごとのデータを保持する日数を指定するオプションをリストから選択し、[Apply] をクリックします。
Monthly aggregated data is kept for (days)	月ごとのデータのトランケーション間隔を設定します。	月ごとのデータを保持する日数を指定するオプションをリストから選択し、[Apply] をクリックします。
Event data is kept for (days)	イベントの履歴データのトランケーション間隔を設定します。	イベント履歴のトランケーション（切り捨て）が実行されるまでの日数を指定するオプションをリストから選択し、[Apply] をクリックします。

表 12-4　システム パラメータの設定（続き）

行の名前	オプション タスク	手順
Task data is kept for (days)	タスクの履歴データのトランケーション間隔を設定します。	タスク履歴のトランケーション（切り捨て）が実行されるまでの日数を指定するオプションをリストから選択し、[Apply] をクリックします。
User Session Polling Interval (hours)	ユーザ セッションのポーリング間隔を設定します。	ポーリング間隔を時間単位で指定するオプションをリストから選択し、[Apply] をクリックします。
User Session Report data is kept for (days)	ユーザ セッション データのトランケーション間隔を設定します。	ユーザ セッション レポートのトランケーション（切り捨て）が実行されるまでの日数を指定するオプションをリストから選択し、[Apply] をクリックします。
Logout User Audit Trail data is kept for (months)	ユーザ監査証跡データのトランケーション間隔を設定します。	ユーザ監査証跡のトランケーション（切り捨て）が実行されるまでの月数を指定するオプションをリストから選択し、[Apply] をクリックします。

ログの操作

Performance Monitor 自体に問題があるという例外的なイベントでは、Performance Monitor のデバッグ ログ ファイルを表示またはダウンロードして、問題の解決のために TAC を利用できます。

また、ログ アウトしたすべての RAS ユーザの VPN セッションを説明している監査証跡も表示できます。

始める前に

このオプションを使用するための適切な権限を持っていることを確認します。ユーザ セッションを終了するには、システム管理者またはネットワーク管理者の必要があります。「ユーザの権限について」（P.3-2）を参照してください。

手順

ステップ 1　[Admin] > [Logs] を選択します。

ステップ 2　TOC からオプションを選択します。

- [Debugging Log Files] をクリックして、Performance Monitor のトラブルシューティングで使用されるログのリストを表示します。このログにはサーバ上の場所や現在のサイズが含まれています。次のデバッグ ログを利用できます。
  - faults.log : *Faults Log* には、障害の履歴データが表示されます。
  - job.log : *Job Log* には、Performance Monitor ジョブの履歴が表示されます。
  - polling.log : *Polling Log* には、displays historical デバイス ポーリング データの履歴が表示されます。
  - validation.log : *Validation Log* には、デバイス ポーリング データの履歴が表示されます。
  - mcpui.log : *Monitoring Center for Performance User Interface Log* には、最近のユーザ インターフェイスのオペレーションが表示されます。
- [Logout User Audit Trail] をクリックすると、ログアウトした RAS VPN ユーザの統計情報が表示されます。表 12-5 に、終了したユーザ セッションを示します。

（注）　ユーザ ログアウト機能については、第 5 章「リモート アクセス VPN サービスのモニタリング」に説明があります。

ステップ 3　（任意）TOC から [Debugging Log Files] を選択した場合、オプション ボタンをクリックしてログを選択し、次のいずれかを実行します。

- HTML バージョンのログを表示するには、[View] をクリックします。
- ログのローカル コピーを保存するには、[Download] をクリックし、表示されたウィンドウで [File] > [Save As] を選択してログをテキスト ファイルまたは HTML ファイルとして保存します。

ログの表示中に [Refresh] をクリックして、最新のポーリング サイクルから情報を表示できます。

参考

表 12-5　[Logout User Audit Trail]

エレメント	説明
[Administrator Name] カラム	記述された VPN セッションを終了した（または終了しようとした）ユーザの CiscoWorks ユーザ名を表示します。 **（注）** ユーザ セッションを終了するには、システム管理者またはネットワーク管理者の必要があります。「ユーザの権限について」（P.3-2）を参照してください。
[Status] カラム	強制的なログアウトに成功したか、失敗したかを示します。
[Error Message] カラム	失敗した場合、関連するエラー メッセージを表示します。 **（注）** 一部の障害は不明なエラーの結果として発生します。このような場合、Performance Monitor でこのカラムにテキストが表示されません。
[Time] カラム	説明した VPN セッションがいつ終了したかを示すタイムスタンプを表示します。
[Logged Out User] カラム	終了した VPN セッションのユーザ名を表示します。
[User Group] カラム	セッションが終了した RAS ユーザに関連付けられた VPN 3000 ユーザ グループの名前を示します。
[Client IP Addr] カラム	VPN に接続されている、説明した RAS ユーザからの IP アドレスを表示します。
[Protocol] カラム	説明した VPN セッションのプロトコルを識別します。
[VPN3K Device] カラム	RAS ユーザが切断された VPN 3000 コンセントレータの DNS 名または IP アドレスを表示します。
[Traffic In] カラム	インバンド バイト数を表示します。
[Traffic Out] カラム	アウトバウンド バイト数を表示します。
[Connection Duration] カラム	VPN トンネルが切断されるまでの合計期間（秒単位）を表示します。
[Throughput (kbps)] カラム	VPN トンネルが切断されるまでの平均スループット速度を表示します。

デフォルト ページの選択

Performance Monitor の起動時にデフォルトで表示されるページを選択できます。デフォルトは [Summary] > [Critical Problems] です。

手順

ステップ 1　[Admin] > [My Profile] を選択します。

ステップ 2　選択ツリーでページ名をクリックし、[Apply] をクリックします。

選択したページは、次回 Performance Monitor を起動したときに最初に表示されます。